ACCESSPRIVACY BY OSLER

Summary Table of Key Elements of Quebec's Proposed Privacy Law Reform, Bill 64, and the General Data Protection Regulation (EU)

In June 2020, the Quebec government tabled Bill 64, An Act to modernize legislative provisions as regards the protection of personal information, which includes significant proposed amendments to an Act Respecting the Protection of Personal Information in the Private Sector (the "Quebec Privacy Act").

Many of the new requirements and individual rights proposed in Bill 64 are similar to those within the General Data Protection Regulation (EU) ("GDPR"). However, in many instances the requirements and other provisions under Bill 64 are more stringent, prescriptive or otherwise distinct from the requirements set out under the GDPR and are unique to the Province of Quebec.

If Bill 64 is enacted in its current form, companies who are subject to the Quebec Act that have established policies, procedures and practices to comply with the GDPR will need to take a series of additional steps to operationalize their compliance with Bill 64 (to the extent it is even practicable to even do so, given the stringent features of many provisions in the Bill). Moreover, Bill 64 exposes companies to significant financial penalties and damages that are even more severe than the potential penalties under the GDPR.

Given the significant compliance costs to comply with Bill 64's unique and stringent requirements and the severe financial risks under Bill 64's enforcement regime, it is reasonable to anticipate that Bill 64 (as currently drafted) will result in many products or services being withdrawn from the Quebec market and some Quebec-based businesses relocating certain of their operations outside the Province.

Commentators have identified multiple ways in which the GDPR has negatively impacted businesses, digital innovation, the labour market and consumers in the EU.[1] By introducing requirements and penalties that go beyond even the GDPR, it is reasonable to anticipate that the impacts in Quebec of Bill 64 will be greater than the impacts in the EU of the GDPR.

The table below summarizes the key differences between Bill 64 and the GDPR and identifies anticipated impacts of these distinctions. The summary comparison table has been prepared in tandem with the Comparison of Key Elements of Bill 64 and the GDPR Table, which provides a more detailed description of the manner in which Bill 64's provisions are more stringent, prescriptive or otherwise distinct from the GDPR.

[1] See for example: What the Evidence Shows About the Impact of the GDPR After One Year (https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/); Regulations like GDPR will make big tech stronger (https://qz.com/1332215/regulations-like-gdpr-will-make-big-tech-stronger/).

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Trans-border Data Flows	Bill 64 provides that, prior to any transborder data disclosure or transfer of data, controllers are required to undertake a privacy impact assessment and only transfer personal information outside Quebec if: (i) the data controller determines that the personal information will receive equivalent protection in the other jurisdiction, and (ii) a written agreement is in place that reflects the results of the privacy assessment and any identified risks. Enterprises may be prohibited from transferring or disclosing personal information to a jurisdiction outside of Quebec that does not have equivalent protections as set out under Bill 64, even if the individual concerned expressly consented to the transfer, or the data controller had previously entered into a written agreement with obligations on the recipient to protect the personal information in a manner consistent with the provisions under Bill 64.	The transborder data flow restrictions under the GDPR are far more flexible, as the GDPR provides for various lawful bases other than adequacy for data controllers to transfer personal data outside the EU, including express consent, Model Clauses, contractual necessity, codes of conduct, and Binding Corporate Rules (Art. 49).	Bill 64's highly restrictive and onerous trans-border data flow provisions may prevent enterprises in Quebec from using many commercially available products and services, including cloud infrastructure, e-commerce solutions, online payment platforms, and customer relationship and marketing tools. Quebec-based multinationals will need to give serious consideration to moving their Quebec-based back office operations used to store and process customer and employee information to another jurisdiction (so that they are able to transfer data within their global operations). Enterprises will incur material expenses and experience significant delays associated with assessing the equivalence of data protection laws in each jurisdiction (including other provinces in Canada) to which they may communicate personal information – something that, as a practical matter, is unworkable.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Confidentiality by Default	Bill 64 requires a data controller who collects personal information when offering a technological product or service to ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned (s. 9.1).	Bill 64's "confidentiality by default" clause is far broader in scope and significantly more stringent than the "privacy by design" concept under the GDPR (which requires the data controller to implement "appropriate technical and organizational measures" for implementing data protection principles in an effective manner, taking into account the nature, scope, context, risks and purposes of processing) (Art. 25(1)). The GDPR also requires data controllers to implement "appropriate" technical and organizational measures to ensure that by default, "only personal data which are necessary for each specific purpose of the processing are processed" (Art. 25(2)).	In many instances, organizations that have implemented "privacy by design" for their product and services in compliance with the GDPR standard will still not be compliant with Bill 64's very stringent "confidentiality by default" requirement. Given the small size of the Quebec market, it is unrealistic to expect that foreign-based technology businesses will create versions of their products and services that are customized to meet the requirements of Bill 64's "confidentiality by default" provision.
Data Impact Assessments	Bill 64 requires enterprises to conduct an assessment of the privacy-related factors of "any information system project or electronic service delivery project". Data controllers will be required to conduct assessments even in circumstances where there may be low or nominal risk associated with the personal information processing activity in question (s. 3.3).	The GDPR requires a data protection impact assessment only where the processing is likely to result in a 'high risk' to the rights and freedoms of natural persons (Art. 35(1)).	Enterprises that carry on business in Quebec will be required to dedicate sufficient resources to perform significantly more impact assessments than if they were not located in Quebec. Given the small size of the Quebec market, businesses located outside Quebec may decide to no longer offer their products or services in the Quebec market.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Consent and other Legal Authority for Processing	Primacy of Consent: Bill 64 enhances the primacy of consent as the default authority for processing personal information under the statute. Separate Consent: Bill 64 requires that consent be requested for each specific purpose, separately from any other information (s. 14). Express Consent: Bill 64 requires express consent for the processing of "sensitive personal information", which is defined as information that "entails a high level of reasonable expectation of privacy" (s. 12). Implied Consent: There is no express provision in Bill 64 for an implied, or assumed, consent for the lawful processing of non-sensitive personal information. Moreover, it is not clear how an implied form of consent can practically be operationalized given the requirement that consent be requested for each specific purpose, separately from other information (as required under s. 14).	Primacy of Consent: Consent is not a primary or default authority for processing personal information. The GDPR sets out other lawful and valid bases for processing of personal data (e.g. contractual necessity, compliance with legal obligations, vital interests, public interest, legitimate interests, or pursuant to a power of a Member state) (Art. 6). Separate Consent: The GDPR does not expressly require that consent be sought separately. Express Consent: The GDPR sets out prescribed categories of sensitive information. Implied Consent: Although the GDPR includes no reference to implied consent, consent is only one of many valid bases for processing of personal data. Expiration of Consent: The GDPR's consent provisions do not expressly address the expiration or other temporal aspects of consent.	Enterprises who are subject to the Quebec Privacy Act that have established policies, procedures and practices to comply with GDPR will need to take a series of additional steps to operationalize their compliance with Bill 64's consent requirements. This will result in businesses incurring material costs and limiting the use of personal information in ways that are permissible under the GDPR.

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
	Expiration of Consent: Under Bill 64, consent is valid only for the time necessary to achieve the purpose for which it was requested (s. 14). Permissible Processing Without Consent: Bill 64 permits the use of personal information as a secondary purpose without the consent of the individual concerned if it is used for purposes "consistent" (a "direct and relevant connection") with the purposes for which it was collected (s. 17, s. 12). Other Exceptions to Consent: Bill 64 requires that personal information used without consent for research or the production of statistics be de-identified (s. 12(3)). Bill 64 does not allow for further processing for archiving purposes in the public interest. Bill 64 sets out that further processing of data for commercial or philanthropic prospection is not permissible (s. 12).	Permissible Processing Without Consent: The GDPR more permissively allows personal data to be further processed for secondary purposes that are not "incompatible" with the initial purposes for its collection (Rec.50; Art.5(1)(b)). A contextual assessment is required to determine the extent of compatibility in the circumstances (Art .6(4)). The GDPR expressly permits the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Art.5(1)(b)). Other Exceptions to Consent: The GDPR does not require "pseudonymization" in all cases in which personal information is used for research and the production of statistics (Art 6(4)(e)). The GDPR does not set out that further processing of data for commercial or philanthropic prospection is not permissible (s.12).	

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Automated Decisions	Bill 64 regulates any decision based exclusively on an automated processing of personal information, with no exceptions (s. 12.1).	Under the GDPR, rules applicable to automated decisions apply only if a decision affects a person's legal status or legal rights or has an equivalent impact on the person's circumstances, behaviour or choices. Additionally, the GDPR provides a number of exemptions, including where an automated decision is necessary for entering into, or performance of, a contract between the data subject and a data controller (Art.22).	Quebec-based businesses will deploy fewer automated (e.g. AI) decision-making processes (due to the necessity of meeting notice, transparency and "decision-review" requirements found in Bill 64, even when a decision has no material impact on the legal status or legal rights of an individual). Quebec may become a less desirable jurisdiction in which to create, scale, operate or invest in businesses that sell or use AI solutions. AI-related research and development activities will be more likely to be performed outside Quebec. There will be fewer new AI-based businesses established in Quebec. There will be an increased likelihood of existing AI-based businesses in Quebec relocating to another jurisdiction.
Deactivation of Identification, Location or Profiling Functions	An enterprise deploying technology that includes functions allowing an individual to be identified, located or profiled must first inform the individual of the use of such technology and the means to deactivate the functions (s. 8.1).	Although a data controller must be transparent about the existence of automated decision-making, including profiling, and provide meaningful information about the logic involved (Art. 13, 2(f)), Bill 64's "deactivation right" appears broader than GDPR's right of objection (Art. 21).	Quebec-based enterprises will be required to incur costs and dedicate resources to implement and manage a deactivation right that is broader than under the GDPR. Technology businesses based outside Quebec will be required to create versions of their products and services that are customized for Quebec to meet these specific requirements.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Take-down, De-indexing and Re-indexing	Bill 64 provides individuals with the right to require cessation of dissemination or de-indexing (s.28.1) if the dissemination contravenes the law or a court order, where certain conditions are met. Bill 64 provides individuals with the right to require re-indexation in the same circumstances where a person may require cessation of dissemination or de-indexing of hyperlinks (Bill 64, s. 28.1). Bill 64 does not provide any exceptions to the rights of cessation of dissemination, de-indexing, and re-indexing.	The GDPR provides individuals with rights of restriction (Art. 18) and objection (Art. 21) and a right of erasure or "right to be forgotten" (Art. 17). The GDPR does not include a right of re-indexation. Under the GDPR, the rights of objection and restriction and erasure are subject to exceptions where the request is manifestly unfounded or excessive, particularly because of its repetitive character. The right of erasure contains further exceptions where processing is necessary for the rights of freedom of expression and information, public health reasons, the performance of a public interest task, and other enumerated reasons (Art. 17).	Enterprises who are subject to the Quebec Privacy Act that have established policies, procedures and practices to comply with GDPR will need to take a series of additional steps and incur material costs to operationalize their compliance with the more stringent take-down, de-indexing and re-indexing provisions under Bill 64.
Data Retention	Prescribed Minimum Retention Period: Bill 64 requires data controllers to retain personal information at least one (1) year where the personal information is used to make a decision (s. 11). Limitation on Retention Period: Bill 64 permits the retention of personal information after the original purpose of the personal information processing is achieved only "where a preservation period is provided for by an Act" (s. 23).	Prescribed Minimum Retention Period: The GDPR does not provide any minimum (or other prescriptive) retention period for personal data and only requires personal data to be retained for "no longer than necessary" (Rec.39; Art.5(1)(e)).	Enterprises that are subject to the Quebec Privacy Act, and that have already established policies, procedures and practices to comply with the GDPR, will need to take a series of additional steps and incur material costs to operationalize their compliance with Bill 64's more stringent data retention requirements.

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
	Anonymization: Where an organization anonymizes personal information after the information is no longer required, the organization must anonymize the data in accordance with "generally accepted best practices" (s. 23). Bill 64 defines "anonymize" in an absolute and stringent fashion as "irreversibly no longer allows the person to be identified directly or indirectly" (s. 23). Transparency of Retention Period: Bill 64 requires that on request an individual must be informed of the duration of the period of time their personal information will be kept (s. 8).	Limitation on Retention Period: The GDPR more flexibly permits data controllers to retain personal data for a broader set of purposes beyond the purposes for which such personal data was initially processed, specifically for purposes that are compatible with such purposes, as well as other specified purposes (see Rec.39; Art.5(1)(e)). Anonymization: The GDPR does not prescribe any standards for anonymization, and the GDPR's definition of "anonymization" appears less stringent than Bill 64 as "anonymous" information for the purposes of the GDPR is information which does not relate to an identified or identifiable natural person, or is rendered anonymous in such a manner that the data subject is no longer identifiable (Rec. 26). Transparency of Retention Period: The GDPR more flexibly requires that when personal data is collected from a data subject, the data controller shall provide the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Art.13(2)(a)).	

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Accountability	An enterprise's CEO or president is required to approve governance policies and practices regarding personal information (s. 3.2) and be directly involved in response to requests for access, rectification and ceasing dissemination or de-indexing (s. 35).	There are no corresponding express obligations on an enterprise's CEO or president.	This accountability provision may significantly raise the personal risk for the CEO or president of an enterprise, as the Quebec Act currently provides that an individual who orders or authorizes an act or omission that constitutes an offense of the data controller under the statute, is deemed to be a party to the offence and is personally liable to prescribed penalties under the Act.
Security Breach Notification	Bill 64 contains a mandatory breach notification obligation to the Commissioner and individuals of "confidentiality incidents" that present a "risk of serious injury" (s. 3.5). Bill 64 defines a "confidentiality incident" to include the communication of personal information "not authorized by law" and (more broadly) "any other breach in the protection of such information."	The notification trigger under the GDPR may set a higher threshold for notification, both in terms of (i) the level of harm to individuals ("high risk" to individuals' rights and freedoms is the test under the GDPR, rather than "risk of serious injury" in Bill 64); and (ii) the definition of a "personal data breach" (which is the comparable term in the GDPR to the broader definition of "confidentiality incidents" in Bill 64) (Art.33).	Enterprises that are subject to the Quebec Privacy Act, and that have already established policies, procedures and practices to comply with the GDPR (or other privacy laws, including PIPEDA) will need to take a series of additional steps and incur material costs to operationalize their compliance with Bill 64's security breach notification requirements.

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Standard for Information Security	Bill 64 contains an absolute requirement for organizations to "protect personal information held by a person", which requires data controllers to establish and implement governance policies and practices that "ensure" the protection of such information (i.e. there is no qualifying concept of reasonable or appropriate security measures) (s. 3.2). These provisions, however, are inconsistent with the qualified requirements set out in section 10, "reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored." (s. 10)	The GDPR's standard for safeguarding is less stringent, as it requires "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (Art.5(1)).	A higher standard for information security in Quebec (combined with the other penalties included in Bill 64) will create incentives for enterprises to limit the personal information that is stored or processed in Quebec. It will also create an incentive for enterprises to move their operations to other jurisdictions.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Penalties	Bill 64 effectively creates no-fault liability under which an enterprise is automatically liable (subject to establishing force majeure) for an injury resulting from the unlawful infringement of rights created by the Quebec Privacy Act or the rights of reputation and privacy set out in the Civil Code of Quebec (s. 93.1). When combined with the Standard for Information Security (s. 3.2), Bill 64 potentially creates a strict liability regime for data breaches. Bill 64 imposes a minimum quantum of punitive damages for intentional or gross fault – $1,000 (s. 93.1). Bill 64's maximum fine may be 8% of worldwide turnover, which is twice the maximum in the EU, notwithstanding that Quebec's population is 2% of the population of EU member countries (s. 92.1). Bill 64 does not cap fines for multiple infringements of different provisions resulting from the same or linked processing activities.	The GDPR does not create strict liability for data breaches. The GDPR does not impose a minimum quantum of punitive damages. The GDPR does not double fines for subsequent offences (e.g., doubling fines from 4% of worldwide turnover to 8% of worldwide turnover). The GDPR caps fines for multiple infringements of different provisions resulting from the same or linked processing activities.	The penalty provisions under Bill 64 is likely to result in significantly more privacy-related litigation in Quebec, including class actions. Quebec-based businesses will need to evaluate whether the increased risk of litigation, and the creation of financial penalties that lack proportionality to the size of the Quebec market, warrant giving serious consideration to relocating the businesses' operation to another jurisdiction.