ACCESSPRIVACY BY OSLER

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

On June 12, 2020, at the National Assembly, 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 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, including the requirements under Bill 64 relating to accountability, a novel "confidentiality by default" requirement, a broad "deactivation" right for identification, location or profiling functions, transborder data flows, data impact assessments, consent and exceptions to consent, the standard for information security, data retention, transparency, automated decision making, and multiple subject matter data rights. In addition, differences in security breach terminology under Bill 64 and the GDPR may result in different standards for the notification trigger under the two statutes, and a lower threshold for notification (and more data incidents being notifiable) under Bill 64 compared to the GDPR. More broadly, unlike the GDPR which provides clarity as to the statutory obligations of data controllers and processors, it is unclear from the drafting of Bill 64 as to precisely which provisions under the Act are intended to apply only to data controllers, or to both controllers and processors.

As such, 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).

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

ACCESSPRIVACY BY OSLER

For clarity, the table below does not list requirements or other provisions that are substantively similar or more permissive than under the GDPR, or that otherwise would not impose an operational burden on an organization whose policies, procedures and practices comply with the GDPR.

For the purposes of this table, references under Bill 64 to a "person carrying on an enterprise" are referred to as "data controllers" (see also Controller vs. Processor).

For ease of reference, you may navigate to a topic of interest using the following Table of Contents:

ACCESSPRIVACY BY OSLER

Summary Table Bill 64 Provisions that are more Stringent, Prescriptive or otherwise Distinct from the GDPR
Accountability - Data Protection Officer/Person in Charge
Senior Executive Responsibility for Data Protection Under Bill 64, the individual who has the "highest authority" (e.g. the Chief Executive Officer or President) is required to exercise the function of a "person in charge" ("PIC") of the data controller's protection of personal information. The Quebec Act currently provides that an individual who orders or authorizes an act or omission that constitutes an offence of the data controller under the statue, is deemed to be a party to the offence and is personally liable to prescribed penalties under the Act. (See s. 93, "Fines, Penalties and Statutory Right of Damages"). The GDPR does not impose a similar responsibility on a data controller's CEO or senior executive. (Art. 37) Approval of Policies and Practices Under Bill 64, the PIC role includes "approving" governance policies and practices regarding personal information. (Bill 64, s. 3.2) Under the GDPR, the DPO is not expressly required to "approve" governance policies and practices. (Art. 37-39)

ACCESSPRIVACY BY OSLER

Delegation of "Person in Charge" Functions

Under Bill 64, the PIC may delegate all or part of that function to a "personnel member", although it is unclear whether the "personnel member" must be an employee of the particular data controller (or whether an employee of an affiliate would be permitted) (Bill 64, s. 3.1). Presumably, any individual who is delegated PIC functions would be exposed to the personal liability provision under the Quebec Act (as described above).

The GDPR permits a group of companies to appoint a single DPO (and as noted above, Bill 64 may not permit this). (Art. 37(3))

Obligations on PIC Regarding Requests for Access, Rectification, De-indexing

Bill 64 specifically required the PIC to be directly involved In response to requests for access, rectification, ceasing dissemination or de-indexing, (Bill 64, s. 35).

The GDPR does not require any particular person to be involved in requests (though see section on DPO generally). (Art. 37)

Accountability - Policies and Practices

Standard for Compliance:

Bill 64 stringently requires organizations to implement governance policies and practices that "ensure" the protection of information. (Bill 64, s. 3.2)

The GDPR sets out a less stringent standard by requiring companies to take "appropriate" measures to demonstrate compliance with the GDPR. (Art. 12(1))

Content of Governance Policies:

Bill 64 requires that governance policies and practices: (i) provide a framework for the keeping and destruction of personal information; (ii) define the roles and responsibilities of the members of its personnel throughout the life cycle of the personal information; (iii) provide a process for dealing with complaints regarding the protection of the personal information; and (iv) are proportionate to the nature and scope of the enterprises activities. (Bill 64, s. 3.2)

These prescriptive content requirements are not expressly contained in the GDPR.

Approval:

Bill 64 requires that governance policies and practices be approved by the PIC. (Bill 64, s. 3.2)

Such an approval is not required by the GDPR.

Adherence to codes of conduct / certification schemes:

Bill 64 does not provide for adherence to an approved code of conduct or certification mechanisms to be used as an element by which to demonstrate compliance, unlike the GDPR. (Art. 24, Rec. 74.)

ACCESSPRIVACY BY OSLER

Controller vs. Processor

While many provisions in Bill 64 refer to "persons carrying on an enterprise" (a concept that includes data controllers), there are multiple provisions drafted with reference merely to "a person" or a "person or body" that suggests that those provisions may apply to both data controllers and data processors. These include:

- "person who collects personal information", regarding individual rights of access and certain notice provisions (ss. 1.1, 8, 8.1 and 8.2);
- "person holding personal information on behalf of person carrying on an enterprise" (s. 16), regarding referring requests for access or rectification;
- "person or body carrying out a mandate or performing a contract of enterprise", regarding the exception to consent related to performance of a contract (s. 18.3);
- "person or body wishing to use the information for study" (s. 21); "person or body wishing to use personal information for study" (s. 21.0.1); and "person who communicates personal information" (s. 21.0.2), regarding the exception to consent related to study/research/statistics;
- "person holding information that is the subject of a request" (s. 36) for access or rectification;
- "person holding the file" (s. 53), in relation to disagreements about requests for rectification;
- "person holding the information" (s. 91), regarding offences.

It is unclear whether these provisions were expressly intended to make a distinction between data controllers and processors, and it is otherwise it's not entirely clear which provisions in Bill 64 that refer to "a person carrying on an enterprise" may apply to processors.

The GDPR provides more clarity about the obligations of controllers vs. processors, by including definitions of "controller" (Art. 4(7)) and "processor" (Art. 4(8)). and specifically enumerates the obligations that apply only to processors (Art. 28).

Data Protection by Design/Confidentiality by Default

Bill 64 contains a broad and very stringent requirement whereby a data controller who collects personal information when "offering a technological product or service must ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned." (Bill 64, 9.1).

The term "confidentiality" is not defined by Bill 64, but the use of the term "confidentiality" in other provisions of the Bill suggests that the concept refers to both security and privacy. As such, this provision appears to require a data controller to implement the "highest level of security and privacy, by default." (Bill 64, 9.1)

Bill 64's "confidentiality by default" clause in section 9.1 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)).

Similarly, 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))

ACCESSPRIVACY BY OSLER

Data Impact Assessments

Bill 64 requires data controllers to conduct an assessment of the privacy-related factors to be undertaken for use of "any information system project or electronic service delivery project". As drafted, data controllers would 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. (Bill 64, s. 3.3).

The GDPR requires a data protection impact assessment ("DPIA") for processing in far less breadth and volume of circumstances, namely only where the processing is likely to result in a 'high risk' to the rights and freedoms of natural persons. (Art. 35(1))

Consent and other Legal Authority for Processing

Structural Differences

Bill 64 enhances the primacy of consent as the default authority for processing personal information under the statute.

Under the GDPR consent is not a primary or default authority for processing personal information, and more clearly 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)

ACCESSPRIVACY BY OSLER

Separate Consent:

Among the requirements for consent, Bill 64 requires that consent be requested for each specific purpose, separately from any other information. (Bill 64, s. 14)

The GDPR does not expressly require that consent be sought separately.

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" (Bill 64, s. 12).

Unlike the GDPR, which sets out prescribed categories of sensitive information, Bill 64 will operationally require a contextual assessment on a case-by-case basis to determine whether express consent would be required in the circumstances.

Implied Consent

While Bill 64 contemplates express consent for the processing of sensitive personal information, 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 that requirement that consent be "requested for each specific purpose, separately from other information (as required under s. 14 of the Bill).

Expiration of Consent:

Under Bill 64, consent is valid only for the time necessary to achieve the purpose for which it was requested. (Bill 64, s. 14)

The GDPR's consent provisions do not expressly address the expiration or other temporal aspects of consent.

Assistance:

Bill 64 requires that if requested, assistance be provided to an individual to understand the scope of consent requested. (Bill 64, s. 14)

This is not required by the GDPR.

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. (Bill 64, s. 17, s. 12)

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)), and a contextual assessment is required to determine the extent of compatibility in the circumstances. (Art .6(4)).

Moreover, the GDPR expressly permits the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, are not considered "incompatible" with initial purposes. (Art.5(1)(b)).

ACCESSPRIVACY BY OSLER

Other Exceptions to Consent:

In regard to the following exceptions to consent, Bill 64 may impose more stringent requirements on organizations than the GDPR:

- The use of personal information for research and the production of statistics (s. 12(3)). Bill 64 requires de-identification (defined at s. 12) for all such uses, whereas the GDPR does not require the equivalent "pseudonymization" in all cases. (Art 6(4)(e)).
- Bill 64 does not allow for further processing for archiving purposes in the public interest, unlike the GDPR (Art. 5(1)(b)).
- Bill 64 sets out that further processing of data for commercial or philanthropic prospection is not permissible (s.12). The GDPR does not.
- Bill 64's exception to consent for the performance of a contract includes requirements to specify measures to protect confidentiality of the personal information (Bill 64, s.18.3), which appear more prescriptive than the requirements for the analogous exception in the GDPR. (Art. 6(1)(b))

Limitation of Collection

Bill 64 prohibits the collection of personal information to circumstance to where it is "necessary" for the purposes determined before collecting it", and contains provisions which suggest that there must be a "serious and legitimate reason" for the collection (ss. 1.1,4, 5).

The GDPR more permissively allows you to collect and process personal data for "specified, explicit and legitimate" purposes (e.g. the purpose for collection does not have to be "serious"). (Art. 5(1)(b))

ACCESSPRIVACY BY OSLER

Security

More Stringent/Unqualified Safeguarding Measures

Bill 64 introduces provisions that impose a very high information security standard that are inconsistent with the unamended information security requirements under the statute.

Specifically, under Bill 64 organizations are required to "protect personal information held by a person" (Bill 64, s. 3.1) and establish and implement governance policies and practices that "ensure" the protection of such information. (Bill 64, s. 3.2)

Bill 64 also requires organizations who collect personal information when "offering a technological product or service must ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned." (Bill 64, s. 9.1)

The information security standards in sections 3.1, 3.2 and 9.1 are inconsistent with the qualified requirements set out in section 10 of the Act which provides that organizations must implement security measures that are "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." (Bill 64, s. 10)

The GDPR's standard for safeguarding is less stringent, as it requires "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." (Art. 5(1))

ACCESSPRIVACY BY OSLER

Approval of Policies and Practices

Under Bill 64, a data controller's policies and practices must be approved by the person in charge of the protection of personal information. (Bill 64, s. 3.2).

There is no requirement under the GDPR for an individual employed or engaged by a data controller to approve information security policies and practices.

Security Breach Notification

Notification of "Confidentiality Incidents"

Bill 64 contains a mandatory breach notification obligation to the Commissioner and individuals for "confidentiality incidents" that present a "risk of serious injury" (Bill 64, s. 3.5).

The definition of a "confidentiality incident" under Bill 64 is different than the definition of a "personal data breach" under the GDPR. In particular, 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 breadth of the phrase "any other breach" and the differences in terminology may ultimately result in a broader set of security incidents being subject to Bill 64's notification regime compared to the mandatory breach reporting regime under the GDPR.

In addition, the notification trigger under Bill 64 ("risk of serious injury") appears substantively similar to the notification trigger concept under the GDPR (which requires notification to individuals where a personal data breach is likely to result in a "high risk" to individuals' rights and freedoms). However, the difference in notification trigger terminology under Bill 64 and the GDPR may result in different standards for the notification trigger, and perhaps a lower threshold for notification (and more data incidents being notifiable) under Bill 64, compared to the GDPR.

No Specific Notification Obligations for Controllers vs. Processors

The notification obligations under Bill 64 apply to "any person carrying on an enterprise" and, unlike the GDPR, do not expressly address the different notification obligations on "controllers" vs. "processors." However, service provider contracts are required to include a requirement for the service provider to notify the outsourcing entity "without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated." (s. 18.3)

Unlike the GDPR, Bill 64 requires that specific criteria be considered in assessing the "risk of injury" and contains a positive obligation to consult the person in charge of the protection of personal information within the enterprise (i.e. Privacy Officer) (Bill 64, s. 3.7).

Requirements to be set out in Regulations

Certain details such as the content of the notifications and record keeping requirements are to be set out in regulations, so it is not yet clear whether they will be more stringent than under the GDPR's Article 33.

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. (Bill 64, s. 11)

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))

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". (Bill 64, s. 23)

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:

Where an organization anonymizes personal information after no longer being required, the organization must anonymize the data in accordance with "generally accepted best practices." (Bill 64, s. 23). Bill 64 defines "anonymize" in absolute and stringent fashion as "irreversibly no longer allows the person to be identified directly or indirectly" (Bill 64, s.23).

The GDPR does not prescribe any standards for anonymization, and the GDPR's definition of "anonymization" is similar but 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 than the data subject is no longer identifiable. (Rec. 26)

Transparency of Retention Period:

Bill 64 requires that on request, from a data processor or controller, an individual must be informed of the duration of the period of time their personal information will be kept. (Bill 64, s. 8)

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))

ACCESSPRIVACY BY OSLER

Transparency

Notice of Policies

Bill 64 requires publication of a data controller's internal governance policies on its website, or if it doesn't have a website, by other appropriate means. (Bill 64, s. 3.2).

The public posting of a data controller's internal governance policies is not required by the GDPR.

Confidentiality Policy

Bill 64 requires any person (i.e. a data controller or processor) that collects information through technological means to publicize a confidentiality policy (and any amendments) on the website, as well as disseminate this policy so it reaches the appropriate person. (Bill 64, s. 8.2). The precise scope of the content of this policy and the circumstances when it would need to be posted is unclear, given the drafting of this provision, and that the term "confidentiality" is not defined under the Bill.

The scope of content in the GDPR for similar transparency requirements is articulated more clearly. (Art. 12-14)

Information About Means of Collection

Bill 64 requires that at the point of collection, an individual must be informed of the means of collection. (Bill 64, s. 8)

The GDPR does not expressly require this type of notice at the point of collection, whether or not the data has been obtained from the data subject: see Art. 13-14).

Transparency and Access Requests

As part of the obligations for a data controller to respond to an access request, Bill 64 requires that on request, a person must be informed of (i) the means of collection of the individual's personal information and (ii) the categories of persons within the enterprise that have access to their personal information. (Bill 64, s. 8)

There is no requirement under the GDPR to provide the above type of information in response to an access request.

Transparency Requirements for Identification, Location and Profiling Technologies

Bill 64 sets out a broad requirement that where personal information is collected through technology that includes functions allowing the person concerned to be "identified, located or profiled", the data controller must first inform the person of the use of such technology, and the means to deactivate the functions that allow a person to be identified, located or profiled. (Bill 64, s. 8.1)

While under the GDPR the controller must be transparent about the existence of automated decision-making, including profiling, and provide meaningful information about the logic involved (see Art. 13, 2(f)), a very broad "deactivation right" seems similar to but potentially broader than the GDPR's right of objection (Art. 21).

ACCESSPRIVACY BY OSLER

Automated Decision Making
Bill 64 requires data controllers who use personal information to render a decision "based exclusively on an automated processing of such information" inform the person concerned. As drafted, this notice requirement would be applicable in all circumstances involving decisions based on automated processing, regardless of materiality of the impact of the decision on the individual. The GDPR's automated decision-making provisions are less stringent, as there are broad transparency obligations on data controllers (unlike a notice requirement under Bill 64) (Art. 13(2)(f)), and the rights of individual to object to the decision apply only where the decision produces "legal effects or has similarly significant effects" on individuals. (Art. 22(1))
Data Accuracy
Bill 64 sets out an unqualified requirement for data controllers to ensure that personal information be up-to-date and accurate when used to make a decision (i.e. there is no limitation as to the time or circumstance when personal information needs to be up-dated) (Bill 64, ss. 11) Under the GDPR the retention requirement is qualified, as personal data must only be kept up to date "where necessary". (Rec.39; Art.5(1)(d))

ACCESSPRIVACY BY OSLER

Transborder Data Flow Requirements

Scope of obligations

Bill 64 contains highly restrictive and very onerous transborder data flow requirements, which apply to disclosures of personal information by a data controller to other data controllers and transfer to third party processors.

The cross-border transfer rules in Bill 64 apply to all disclosures and transfers of personal information outside Quebec (including transfers to other provinces and territories within Canada), (Bill 64, s. 17), unlike the GDPR which only restricts transfers to countries or territories outside the EEA. (Art. 45)

Requirement for Privacy Impact Assessment

Bill 64 provides that, prior to any transborder data disclosure or transfer, 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.

Equivalence of Protection in other Jurisdictions

Bill 64 provides that the Minister may publish a list of jurisdictions with equivalent protection, although it is unclear as to whether a privacy impact assessment and/or a written agreement that reflects risks (as described above) would still be required for transfers of personal information to jurisdictions contained on this list. (Bill 64, s.17.1)

ACCESSPRIVACY BY OSLER

Lack of Lawful Authority for Transborder Data Flows where no Equivalency

As drafted, data controllers would be prohibited under Section 17 of Bill 64 from transferring or disclosing personal information to a jurisdiction outside of Quebec that did 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)

Right of Access

Notice of Right:

Bill 64 provides that any person (i.e. a data controller or a processor) who collects personal information from a person must inform that person of the rights of access and rectification provided by law. (Bill 64, s. 8)

The GDPR right of access provisions apply only to data controllers, and requires that at the time when personal data is collected from a data subject, the controller provides the existence of the right to request access to, rectification of or erasure of personal data, or restriction of processing concerning the data subject. (Art. 13(2)(b))

Scope of right:

Under Bill 64 every person (i.e. a data controller or a processor) who holds personal information on another individual, must confirm the existence of the personal information and allow the individual to retain a copy of it. (Bill 64, s. 27)

The GDPR provides that a data controller (but not a process) shall provide confirmation as to whether the individuals' personal data has been processed, and access to the personal data and prescribed details. (Art. 15(1))

Under Bill 64, requests for access may be made by a person who provides that they are the person concerned, their representative, heir or successor and other specified persons: see Bill 64, s. 30. The GDPR has no equivalent requirement, and allows access to the individual only.

Form of Response:

Bill 64 provides that upon request, computerized personal information must be communicated in the form of a "written and intelligible transcript." (Bill 64, s. 27) If the person concerned is handicapped, "reasonable accommodation" must be provided upon request. (Bill 64, s. 27)

Under the GDPR, the information must be provided in a "commonly used electronic form" when responding to a request by electronic means. (Art. 15(3))

Timing of Response

Bill 64 requires a response by PIC to requests for access 'promptly' and no later than 30 days (Bill 64, s. 32). There is no provision allowing this time period to be extended.

(The GDPR is 'without undue delay' and in any event within 1 month: see Art. 12(3)).

The GDPR allows, with respect to similar rights, for extension of 2 months where necessary, having regard to the complexity and number of requests (Art. 12(3)).

Person in Charge:

See the Person in Charge section for other obligations about subject matter rights requests and timing requirements.

Refusals:

Under Bill 64, any refusal to grant a request must be accompanied by reasons for refusal and an indication of the provision of law on which the refusal is based, the remedies available to the applicant, the time limits for exercising them, and on request help in understanding the refusal. (Bill 64, s. 34)

Under the GDPR, where a data controller intends to refuse to respond to a request, the data controller less prescriptively is obligated only to give reasons where they do not intend to comply with access requests. (Rec. 59)

Deceased Persons:

Under Bill 64, an individual may be able to access the personal information concerning a deceased person, if they are the spouse or close relative of the person if knowledge of the information could help the applicant in the grieving process and if the deceased person did not record in writing his refusal to grant such a right of access. (s. 40.1)

Data relating to deceased persons generally falls outside the scope of the GDPR (except to the extent it also relates to a living person).

Right of Data Portability

Bill 64's provisions setting out the scope of the right of access generally apply to the right of data portability. The following differences between Bill 64 and the GDPR are notable as potentially providing a more expansive right of portability in the Quebec context compared to the GDPR (Art. 20):

- Bill 64's right of portability applies in all cases to provided computerized information, unless doing so raises serious practical difficulties (Bill 64, s. 27). The GDPR limits the portability right to the following circumstances:
    - the individual 'provided' (this is interpreted widely by supervisory authorities to include 'observed' data, but not so far as inferred or derived data) the personal data in the first place;
    - the data is automated (i.e. no paper records); and
    - the basis for processing of the data is consent or to fulfil a contract or steps preparatory to a contract.

- The GDPR provides a portability right to the individual only. Bill 64 permits a wider range of people to submit requests, including representatives, heirs, and successors (see Bill 64, s. 30).
- Bill 64 provides a portability right with respect to data relating to deceased individuals (Bill 64, s. 40.1). Data relating to deceased persons generally falls outside the scope of the GDPR (except to the extent it also relates to a living person).
- Unlike Bill 64, under the GDPR, there is an exception to the right of portability where a request is manifestly unfounded or excessive, particularly because of its repetitive character, the controller may refuse to act on the request or charge a reasonable fee (Art. 12(5)).

Right of Rectification

Scope of Right

Bill 64 permits a wide range of people to submit requests for rectification, including representatives, heirs and successors (Bill 64, s. 30). The GDPR provides a right of rectification to the individual only. (Art. 16)

Bill 64 provides rectification rights with respect to data relating to deceased individuals (Bill 64, s.30). Data relating to deceased persons generally falls outside the scope of the GDPR (except to the extent it also relates to a living person).

Bill 64 provides a rectification right with respect to equivocal data or where keeping or collecting it is not authorised by law, in addition to inaccurate or incomplete data (Bill 64, s.28). The GDPR's rectification right is limited to inaccurate or incomplete data. (Art. 16)

Bill 64's right to have incomplete personal data completed is not limited having regard to the purpose of the processing, unlike the GDPR. As such, Bill 64 more broadly requires processors to take steps to rectify the personal information regardless of the purpose of the processing, whereas the GDPR requires that the purpose be taken into account. (Art. 16)

Burden of Proof:

Bill 64 requires the person holding the file, in case of disagreement, to prove that the file need not be rectified, unless the information was communicated to him by the person concerned or with their consent (Bill 64, s. 53)

The GDPR does not expressly address the burden of proof on the controller (though under the accountability principle a controller must be able to demonstrate compliance with the accuracy principle).

Person in Charge and Timing:

See the Right of Access section for obligations for requests and timing requirements.

Exceptions:

Bill 64 does not provide any exceptions to the right of rectification unlike the GDPR and Member State national laws.

Rejection:

Bill 64, unlike the GDPR, requires the person in charge to:

- indicate the provision of law on which refusal is based;
- inform the requestor of the time limit for exercising remedies; and
- on request, help the requestor understand the refusal. (Bill 64, s. 34)

ACCESSPRIVACY BY OSLER

Rights of Restriction, Objection and Erasure (GDPR) vs. Right to Cessation of Dissemination, De-indexing, and Re-indexing (Quebec Bill)

Scope of right

There is a right in Bill 64 to require **cessation of dissemination or de-indexing** (Bill 64, s. 28.1), if the dissemination contravenes the law or a court order, where certain conditions are met. The GDPR does not contain such rights, but does contain **rights of restriction** (Art. 18) and **objection** (Art. 21) and a **right of erasure or "right to be forgotten"** (Art. 17), which may achieve the same outcomes.

Comparing the scope of the rights:

- The right to require cessation of dissemination or de-indexing in Bill 64 arises in different circumstances to the rights of restriction, objection and erasure in the GDPR. Under Bill 64, the person may require cessation of dissemination or de-indexing of hyperlinks where:
    - the dissemination of the information causes the person concerned serious injury in relation to his right to the respect of his reputation or privacy;
    - the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and
    - the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury. (Bill 64, s. 28.1)

- In contrast, under the GDPR:
    - the **person may require restriction** in certain circumstances involving contested accuracy, the exercise or defence or legal claims, or where the controller is verifying whether to stop processing, in which cases the data can be stored but not used: see details at Art. 18;
    - the **right to object** to processing can be exercised in circumstances involving direct marketing, processing for scientific, historical research or statistical purposes, or legitimate interest or public interest legal basis, subject to certain exceptions for public interest tasks or compelling legitimate grounds: see Art. 21;
    - the **right to erasure or to be forgotten** (Art. 17) can be exercised in any of a number of situations, including withdrawal of consent and there is no other lawful basis, or the data is no longer necessary for the purposes for which it was collected/processed.
- There is also a right in Bill 64 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). There is no such right in the GDPR.
- Bill 64 permits a wider range of people to submit requests for cessation of dissemination, indexing or re-indexing, including representatives, heirs or successors (Bill 64, s. 30). The GDPR provides a right of restriction, erasure and objection to the individual only. (Art. 17, Art. 18, Art. 21).

Person in charge (PIC)

See the Right of Access section for obligations for requests and timing requirements.

Exceptions

Bill 64 does not provide any exceptions to the rights of cessation of dissemination, de-indexing, and re-indexing, unlike the GDPR and Member State national laws with respect to similar rights. Under the GDPR, the rights of objection and restriction and erasure contain exceptions where the request is manifestly unfounded or excessive, particularly because of its repetitive character. The rights 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: see Art. 17.

Rejection of Request

For refusals to cease dissemination, de-index or re-index, Bill 64, unlike the GDPR, requires the person in charge to:

- indicate the provision of law on which refusal is based;
- inform the requestor of the time limit for exercising remedies; and
- on request, help the requestor understand the refusal. (see Bill 64, s. 34)

ACCESSPRIVACY BY OSLER

Fines, Penalties and Statutory Right of Damages

Categories of Fines and Penalties

Under Bill 64, there are two types of monetary penalties:

1. **fines** of up to CAD $25 million, or if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year, on the commission of certain offences (Bill 64, s. 91); and

2. **administrative monetary penalties ("AMP")** of up to CAD $10 million, or if greater, the amount corresponding to 2% of the organization's worldwide turnover for the preceding fiscal year, for enumerated infringements (Bill 64, s. 90.12).

These mirror the two brackets of fines set out in the GDPR (at Art. 83), based on the seriousness of the infringement:

1. **More serious infringements** are subject to a maximum fine of €20m, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

2. **Less serious infringements** are subject to a maximum fine of €10m, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Scope of Fines and Penalties

Despite the analogous categories, penalties are potentially more onerous under Bill 64 than the GDPR:

- **Potentially higher penalties for equivalent infringements:** For example, under the GDPR, failure to comply with the consent requirements when offering information society services directly to a minor is classified as a less serious infringement (Art. 83(4)). Under Bill 64, the use of personal information in contravention of any part of the Act (which would include failure to comply with the consent requirements for minors) is subject to a maximum fine of the greater of $25m or 4% of global turnover (Bill 64, s. 91). However, under Bill 64 'turnover' is based upon the legal entity in question and does not, unlike the GDPR, extend to the wider economic unit. This means a GDPR fine could still be higher in some cases.
- **Unique offence of "re-identification".** Under Bill 64, anyone commits an offence who identifies or attempts to identify a natural person using de-identified information, without the authorization of the person holding the information or using anonymized information, and is liable to fines (Bill 64, s. 91(3)). There is no specific equivalent offence under the GDPR.
- **Automatic doubled fine for subsequent offences:** Under Bill 64, in the case of a subsequent offence, the fines are automatically doubled (Bill 64, s. 92.1). Under the GDPR, relevant previous infringements are taken into account in setting the quantum of the fine, but there is no automatic increase. Where the fine is doubled due to a previous infringement, the maximum fine under Bill 64 is higher than that under the GDPR (8% vs. 4% of global turnover), although, as mentioned above, turnover is computed differently for the purposes of the GDPR.
- **No cumulative cap:** Under the GDPR, where the same or linked processing activity infringes several provisions, the fine will not exceed the specified amount for the gravest breach. While Bill 64 limits cumulative fines for infringement of the same provision, no cap is set out for multiple infringements of different provisions resulting from the same or linked processing activities.
- **Minimum fines:** Bill 64 provides for a minimum fine for offences under the Act of $5,000 for natural persons and $15,000 for organizations (Bill 64, s. 91). The GDPR does not set out any minimum fines.

- **Personal liability:** The Quebec Act already sets out personal liability for the administrator, director or representative of the person who ordered or authorized the act or omission constituting the offence and exposes individuals to the prescribed penalties under the Act. Bill 64 did not change this provision (s. 93), but drastically increases the personal exposure. The GDPR does not set out personal liability in this way, though Member State national laws may potentially do so.

- **Criteria for Quantum of Penalties:** In setting an AMP or fine, Bill 64 may, in some cases, be potentially more stringent than the GDPR. In particular, the framework criteria guiding the decision to impose an AMP under Bill 64 (s. 90.2(2)) differs from the GDPR criteria at Art. 83 in the following respects, including:

    - the Commission may take into account "risk" of prejudice under Bill 64 framework, whereas, under the GDPR, only actual damage is to be taken into account;

    - Bill 64 framework does not take account of whether or not the PIC/controller has adhered to an approved code of conduct;

    - Bill 64 framework does not include a catch-all for other aggravating/mitigating factor;

    - Bill 64 framework takes into account the measures taken to remedy the "failure", whereas the GDPR focuses on measures taken to remedy the "damage".

- **Appeals to provincial Court of Quebec.** Appeals under Bill 64 are to the provincial Court of Quebec rather than the Superior Court (see s. 90.9, re: AMPs). Moreover, s. 90.9 provides that sections 61 to 69 of the current Act will govern the contestation of the monetary administrative penalty. This entails that appeals are only possible on questions of law or jurisdiction (s. 61) and that the decision of the judge of the Court of Québec is without appeal (s. 69). As such, the only avenue for further contestation would be through judicial review to the Superior Court, with a very limited scope of possible intervention by that Court and further appellate Courts. These limited recourses are concerning considering the potential scope of monetary administrative penalties that could be at issue, which amounts would far exceed the normal jurisdiction of the Court of Québec, which in civil matters is limited to claims under $85,000, and even then with full appeal rights to the Québec Court of Appeal.

Statutory damages basis of compensation:

Bill 64 provides a statutory right of damages compensating for injury (s. 93.1). Under the GDPR, the right to compensation is for "material or non-material damage" suffered. (Art. 82)

Controller only:

Bill 64 does not provide for liability for damages by processors, unlike the GDPR, which provides that a processor shall be liable for the damage caused by processing, but only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. (Art. 82)

Exemption from liability:

Bill 64 contains a different, arguably more limited test for exemption from liability ("superior force") than the GDPR ("not in any way responsible").

Minimum / punitive damages:

Bill 64 imposes a minimum quantum of punitive damages for intentional or gross fault ($1,000: see Bill 64, s. 93.1). The GDPR does not.

Joint responsibility:

Bill 64 does not address where there is more than one party responsible or provide for the possibility to recoup damages from processors or other controllers involved in the same processing. The GDPR addresses this joint responsibility at Art. 82.