


The background of the entire page is an abstract digital composition. It features a grid of squares in various colors including yellow, orange, blue, and purple. Overlaid on this grid are numerous thin, glowing lines in blue and orange, creating a sense of depth and movement. There are also clusters of small, bright blue dots scattered throughout the design.


mccarthy
tetrault

Québec Privacy Compliance Toolkit

Navigating a New Regime under Law 25
(formerly Bill 64)

mccarthy
tetrault



 This article is for general information only
and is not intended to provide legal advice.

Law 25 Compliance Toolkit

1 Introduction

On September 22, 2021, the Act to Modernize Legislative Provisions respecting the *Protection of Personal Information* (“**Law 25**”, formerly known as Bill 64) received royal assent.

The passage of Law 25 overhauled Québec’s privacy regime and will have major consequences for businesses that do business in the province or handle the personal information of Québec residents. Aimed at promoting transparency and enhancing data privacy, the significant changes to the existing *Act Respecting the Protection of Personal Information in the Private Sector*, as amended by Law 25 (collectively, the “**Private Sector Act**”) include more stringent obligations for businesses, greater accountability and tougher penalties for non-compliance.

So what does this mean for your business? Ensuring compliance requires careful planning and a thorough understanding of this unique “made in Québec” approach to privacy protection. Law 25 will require businesses to review their practices and processes that relate to the collection and use of personal information. Many existing practices will not comply with the new requirements created by Law 25 and businesses need to adjust accordingly. Law 25 has created new penalties for non-compliance, including massive monetary penalties.

This toolkit is designed to help you comply with Law 25. It will allow your business to understand the new layer of regulation that Law 25 has added on top of prior federal and provincial obligations. More than ever before, businesses must master the legal and regulatory framework that surrounds personal information. This toolkit will help you and your business define your compliance journey.

Table 1: Summary of Amendments and Timeline of Entry Into Force Dates

September 22, 2022: New Obligations	September 22, 2023: New Obligations	September 22, 2024: New Obligations
<ul style="list-style-type: none">✓ Appointment of a Privacy Officer✓ Mandatory Breach Reporting✓ Consent Exceptions for:<ul style="list-style-type: none">• Commercial Transactions; and• Study, Research, or Statistics✓ Disclosure of biometric databases and the uses of biometrics for authentication to the CAI	<ul style="list-style-type: none">✓ Privacy Framework✓ Additional transparency requirements✓ Privacy Impact Assessments✓ Privacy by default and by design✓ De-indexation rights✓ Additional consent requirements✓ Cross-border transfers of personal information (“PI”)✓ New regime for the secondary use of PI✓ Strict PI retention and destruction obligations✓ New obligations when an automated decision is made using an individual’s PI✓ New regime for business contact information✓ New sanctions for non-compliance	<ul style="list-style-type: none">✓ Right to Data Portability

2 Introduction of monetary administrative penalties

One of the major changes introduced by Law 25 is the introduction of a regime that provides for the imposition of significant monetary administrative penalties. This regime will be implemented on September 22, 2023.

This regime gives the Commission d'accès à l'information (the "**Commission**" or "**CAI**") the power to impose monetary administrative penalties, in order to promote the achievement of the objectives pursued by the Private Sector Act, to encourage businesses to quickly take the necessary remedial measures in the event of a failure, and to deter repetition of such failures. The Commission is empowered to impose monetary administrative penalties for a very wide range of contraventions under section 90.1 of the Private Sector Act.

The amount of monetary administrative penalties imposed on a company could be up to \$10 million, or, if greater, up to 2% of worldwide turnover for the preceding fiscal year. These amounts are comparable to those provided for in the European Union's *General Regulation on Data Protection* ("**GDPR**").

Law 25 also grants the Commission the right to institute penal proceedings for an offence under the Private Sector Act. As such, the Commission's attorneys may institute penal proceedings before the Court of Québec, similar to the role played by the Director of Criminal and Penal Prosecutions. These penal proceedings could lead, for corporations, to fines ranging from \$15,000 to \$25 million, or, if greater, up to 4% of the previous year's worldwide turnover.

In addition to providing for significant monetary administrative penalties and fines, Law 25 provides that a breach of the Private Sector Act could give rise to an award of punitive damages in the event of gross fault or intentional infringement. In Québec, in order to claim punitive damages, it must be specifically provided for by a statute. Here, the legislator facilitates the claim for punitive damages for individuals who suffer harm as a result of a breach of the Private Sector Act. An individual may claim \$1,000 or more in punitive damages in such a case, with the potential of individual claims combining in a class action.

Table 2: Summary of Penalties for Individuals and Businesses

Administrative Monetary Penalty (Max)	Penal Offence (Max)	Civil Damages
For businesses/corporations: \$10,000,000 or 2% of worldwide turnover for the preceding year	For businesses/corporations: \$25,000,000 or 4% of worldwide turnover for the preceding year	\$1,000 minimum damages
For individuals: \$50,000	For individuals: \$100,000	

The Private Sector Act stipulates that the decision to impose monetary administrative penalties and their amount will be assessed by the Commission based on several criteria, including:

- The nature, seriousness, duration, and repetitiveness of failures
- Sensitivity of the personal information concerned
- The number of persons concerned and the risk of prejudice to which they are exposed
- The person in default's ability to pay

A business' response to contraventions will also have a significant impact on the Commission's assessment of the appropriate sanction. The Private Sector Act provides that the Commission may consider measures already taken by businesses to remedy the contravention or mitigate its consequences, the degree of cooperation offered to the Commission, and the compensation already offered by businesses to persons whose personal information is compromised.

The new enforcement powers of the Commission, when combined with extraordinarily high levels of potential administrative monetary sanctions, fundamentally changes the risk calculus associated with privacy compliance in Québec.



3 Governance and accountability

Law 25 makes notable governance-related amendments to the Private Sector Act requiring action from businesses, including:

- appointing a "Person in Charge of Personal Information" (the "**PCPI**") within the business, such as a Chief Privacy Officer;
- establishing and publishing governance policies and practices with respect to personal information;
- conducting a privacy impact assessment ("**PIA**") for the development, acquisition, or redesign of electronic service delivery projects involving personal information; and
- establishing response procedures for rights-based requests made by individuals whose personal information may be collected.

A. DESIGNATION OF A PCPI

Starting September 2022, each business must designate a PCPI who will be responsible for protecting personal information and ensuring that the business implements and complies with the Act (s. 3 of the Private Sector Act). By default, the PCPI is the person exercising the highest authority within the business. However, he or she may delegate all or part of that function to any individual, whether working for the company or not, thus allowing businesses to outsource this function to a specialized person.

The title and contact information of the PCPI must be available to the public either on the business' website or by any other appropriate means (s. 3.1 of the Private Sector Act).

Table 3: Examples of PCPI responsibilities

<p>Compliance Duties/Efforts</p> <ul style="list-style-type: none"> – Compliance related to privacy, security, confidentiality – Ensure both existing and new services comply with privacy and data security obligations – Ensure the business has and maintains appropriate privacy and confidentiality consent, authorization forms, information notices and materials reflecting current organization and legal practices and requirements – Operationalize compliance efforts <ul style="list-style-type: none"> – Maintain current knowledge of applicable privacy laws and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance <p>Intra-organizational Collaboration</p> <ul style="list-style-type: none"> – Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues – Collaborate on cyber privacy and security policies and procedures – Work cooperatively with business units in facilitating consumer information access rights – Serve as the information privacy liaison <p>Incident Response</p> <ul style="list-style-type: none"> – Mitigate effects of a use or disclosure of personal information by employees or business partners – Administer action on all complaints concerning the business’ privacy policies and procedures in coordination and collaboration with the leadership team and, when necessary, legal counsel <p>Employee Training</p> <ul style="list-style-type: none"> – Conduct ongoing privacy training and awareness activities 	<p>Data Governance</p> <ul style="list-style-type: none"> – Assure that the technologies maintain, and do not erode, privacy protections on use, collection and disclosure of personal information – Conduct adequacy assessments to ensure that any cross-border data transfers offer sufficient protection to the personal information involved – Conduct periodic privacy impact assessments and ongoing compliance monitoring activities – Account for and administer individual requests for release or disclosure of personal and/or protected information <p>Third Party Contracts</p> <ul style="list-style-type: none"> – Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements – Ensure that written agreements with data processors appropriately address risks identified in privacy impact assessments – Work with counsel relating to business partner contracts <p>Build & Improve the Privacy Program</p> <ul style="list-style-type: none"> – Develop and coordinate a risk management and compliance framework for privacy – Develop and manage business-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations – Establish a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the business’ privacy policies and procedures – Lead the planning, design and evaluation of privacy and security projects – Establish an internal privacy audit program – Periodically revise the privacy program in light of changes in laws, regulatory or company policy
---	---



B. PUBLICATION OF GOVERNANCE POLICIES AND PRACTICES REGARDING THE PROTECTION OF PERSONAL INFORMATION

Businesses will now have to maintain governance policies and practices aimed at protecting personal information that need to be proportionate to the nature and scope of their activities. These policies must be drafted in a clear manner and published by appropriate means by the business, including on the business's website. Some baseline requirements that will need to be addressed in a governance policy include:

- a framework for the retention and destruction of personal information;
 - Under s. 23 of the Private Sector Act, a business must destroy or anonymize personal information when the purposes for which such information was collected or used are achieved.
- defined roles and responsibilities for personnel throughout the life cycle of the personal information held;
- a process for dealing with complaints regarding the protection of personal information held; and an obligation to publish the privacy policy and subsequent amendments on their website.

C. PRIVACY IMPACT ASSESSMENTS

There are two different circumstances under which Law 25 imposes an obligation to conduct a PIA.


First, Law 25 requires businesses to conduct an assessment of privacy-related factors in any project to acquire, develop, or overhaul an information system or electronic service delivery system involving personal information (s. 3.3 of the Private Sector Act).

The PIA must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

In addition, the project must be able to accommodate data portability – an individual's right to receive information in "a structured, commonly used technological format" (See section 4(d) – [Rights Based Requests](#)).

The PCPI may, at any stage of such a project, suggest the implementation of personal information protection measures to help mitigate any identified risks.

Second, Law 25 creates a requirement to conduct a PIA before information can be disclosed outside of Québec (s. 17 of the Private Sector Act). This obligation applies to



both inter-provincial and to foreign disclosures. The PIA must include at least an assessment of these privacy-related factors:

- i. the sensitivity of the information;
- ii. the purposes for which it is to be used;
- iii. the protection measures, including those that are contractual, that would apply to it; and
- iv. the legal framework applicable in the State in which the information would be disclosed including the personal information protection principles applicable in that State.

The information may be communicated if the assessment establishes that it would receive **adequate protection**¹, in light of generally recognized principles regarding the protection of personal information. The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.

The same uncertainty applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on its behalf.

¹ The “adequate protection” threshold assessment is fraught with difficulties. Businesses have to make their own assessments as to whether information would receive “adequate protection”.

For example, it is unclear what “generally recognized principles regarding the protection of personal information” means. Does this refer to the laws of Canada, the EU, or another country? Would meeting the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data be sufficient? Would meeting the privacy standards in trade agreements such as The Council of Europe’s Modernized Convention on Personal Data Protection meet the standard?

In this regard, it is important to note that Law 25 does not adopt any of the GDPR-concepts such as standard contractual clauses, binding corporate rules, a way for the Province to make findings of adequacy, or formal safe harbour mechanisms.

Law 25 requires businesses to mitigate some risks through contractual controls. However, the Commission’s expectation on the level of mitigation through technical, administrative, or physical controls remains unclear.

D. RIGHTS-BASED REQUESTS

Businesses should develop processes to facilitate their responses to the rights-based requests introduced by Law 25. This includes drafting policies and mapping out procedures to respond in a timely manner to requests for access, rectification, de-indexation/re-indexation/cessation of dissemination, and data portability.

i. Right of access and rectification

Under Law 25, a business that collects personal information must inform the person concerned of their rights of access and rectification when the information is collected and subsequently on request. An individual can request to rectify his information if it is “inaccurate, incomplete or equivocal” (s. 28) or if the collection, communication or use of the information is not authorized by law. In light of this requirement, businesses should revise their external and internal privacy policies to inform individuals and employees about their right to access or rectify the personal information that the business holds about them.

ii. Right to control the dissemination of personal information

Starting on September 22, 2023, individuals will have a right to control the dissemination of their personal information by businesses. Individuals can either request the business to cease disseminating their personal information or de-index any hyperlink providing access to the information if the dissemination contravenes the law or a court order, or causes serious harm to the reputation or privacy of an individual. Accordingly, businesses should implement processes to help them determine whether the continued dissemination of the information might result in an injury, whether that injury outweighs the public’s right to information and the freedom of expression of the publisher, and whether the remedy being requested is not excessive in terms of preventing the perpetuation of the injury. To make this assessment, the business must consider a number of prescribed factors which include: the public status of the individual; whether the information concerns a minor; the accuracy and sensitivity of the personal information, the context of its dissemination; the time elapsed since it was published; and lastly if the information is linked to criminal matters, the existence of a pardon or restriction on the access of criminal records.



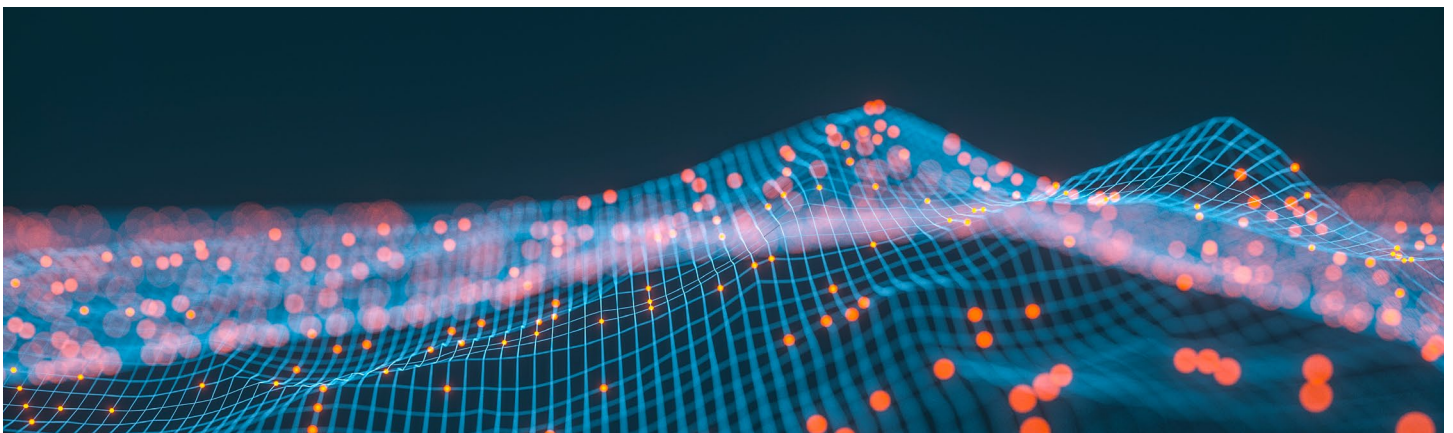
Procedure for the right of access and rectification and the right to control the dissemination of personal information:

1. **Businesses will only need to consider requests made in writing by a person who proves that the personal information relates to them.**
2. **All requests must be made to the PCPI. If the request is not sufficiently precise, the PCPI should assist in identifying the information being sought.**
3. **The PCPI must reply in writing to the request no later than 30 days from the receipt of the request (s. 32). However, the business may submit a request to the Commission within this initial 30-day period to extend the time limit within which it must provide its response (s. 46).**
4. **In case the request is refused, the PCPI must provide reasons and indicate the provision of law on which the refusal is based, the remedies available to the applicant and the time limit for exercising them. If the applicant so requests, the person in charge must also help him understand the refusal (s. 34).**
5. **The business must inform the applicant of their right to submit an application for the examination of a disagreement to the Commission within 30 days of the refusal to grant the request (s. 43).**
6. **The Commission has the power to prescribe a particular course of action with which a business will have to comply in 30 days.**

iii. Right to data portability

As an extension of the right of access, the Private Sector Act grants individuals an additional right to have a copy of computerized personal information collected from them. The information should be in a structured, commonly used and technological format and communicated in a form of a written and intelligible transcript. Individuals can request to have this information transferred directly to “any person or body authorized by law to collect such information” (s. 27 of the Private Sector Act). Businesses are exempted from responding to a data portability request if it, “raises serious and practical difficulties” (s. 27 of the Private Sector Act).

Businesses have until September 2024 to define and implement a process to export personal information collected or stored digitally and to receive such data from another business.



4 Consent

Consent was a cornerstone of the previous version of the Private Sector Act and this principle is reinforced in the reform introduced by Law 25. In the amended Private Sector Act, consent requirements are closely related to transparency requirements.

A. WHAT DO BUSINESSES NEED TO INFORM INDIVIDUALS ABOUT PRIOR TO COLLECTION?

Prior to Law 25, the Private Sector Act required private sector businesses to disclose, prior to collection, the purpose for collecting personal information, the use of personal information, the location of the personal information, and the individual's right to access and correct the personal information (s. 6 of the Private Sector Act). The amended version of the Private Sector Act introduces increased transparency requirements. If the information is collected by technological means, the business must publish a privacy policy on the company's website and disseminate it to reach the persons concerned (s. 8.2 of the Private Sector Act). Under Law 25, private sector businesses now need to inform individuals of:

- **The purposes for which the information is collected** (s. 8(1) of the Private Sector Act). Businesses must transparently disclose the purposes for which personal information is collected.
- **The rights of access and rectification provided by law** (s. 8(3) of the Private Sector Act), which was already in force under the past version of the law.
- **The person's right to withdraw consent to the communication or use of the information collected** (s. 8(4) of the Private Sector Act). This new right does not mean that businesses need to re-obtain consent that was obtained before the passage of Law 25. If an individual agreed to a particular use of personal information prior to Law 25's entry into force, the consent is still valid under the presumption that it was obtained in adherence to the previous Act's then existing provisions.
- **The names and/or categories of the third persons that will have access to the information** (s. 8 of the Private Sector Act), for example if the personal

information is collected for a third person or if communicating the personal information to third persons is necessary for the purposes of the collection.

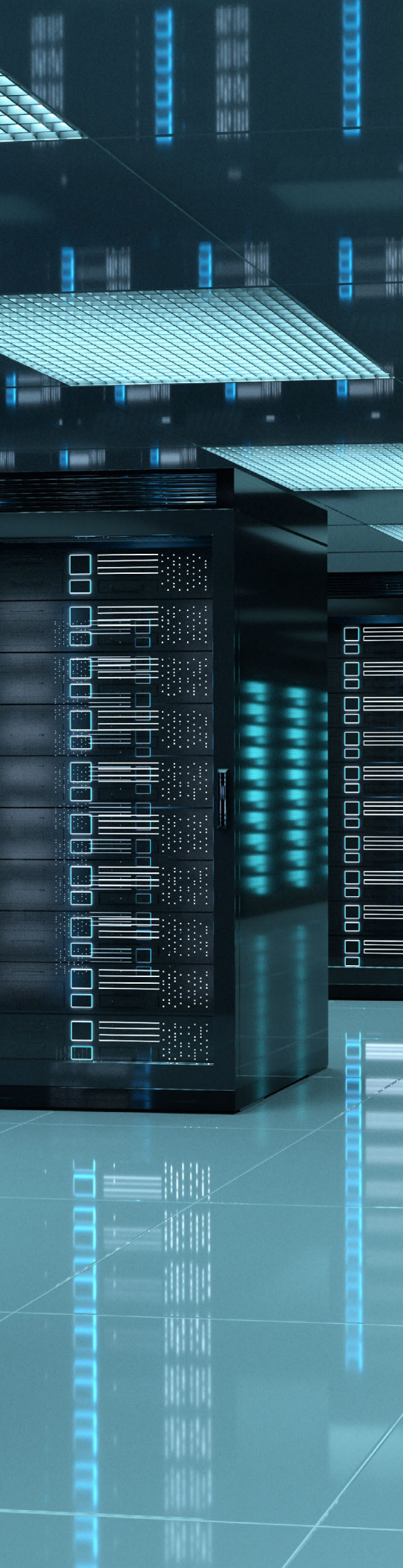
- **The use of profiling, locating or identifying functions** (s. 8(2) of the Private Sector Act). If the technology used to collect personal information uses profiling, locating or identifying functions, individuals must be informed of the use of this technology and the functions that allow the technology to be activated (see s. 8.1 of the Private Sector Act; and section 7 – Privacy by Design).
- Finally, **the possibility that the information could be communicated outside of Québec** – including other Canadian provinces – must be disclosed to the individuals involved (s. 17 of the Private Sector Act).

Law 25 also allows individuals to request additional information. Thus, if requested by the person concerned, businesses need to disclose:

- The contact information of the PCPI (see section "3 – Governance and Accountability")
- The duration of time the personal information will be kept;
- What personal information is collected from the individual; and
- The categories of persons who have access to the information within the business.

B. HOW SHOULD BUSINESSES INFORM INDIVIDUALS WHEN OBTAINING CONSENT?

The obligation to obtain consent directly from the person they are collecting the personal information from remains unchanged, as well as the corresponding exceptions (s. 5 of the Private Sector Act). However, if the business is collecting the consent of a minor under 14 years of age, it has to obtain it from the person having parental authority or by the tutor (s. 14(2) of the Private Sector Act).



Moreover, businesses are required to use clear and simple language in their privacy policies (s. 3.2 of the Private Sector Act). If the communication is made in writing, it must also be presented separately from any other information (s. 14 of the Private Sector Act). As a result, privacy policies cannot form part of more general documents, such as terms of service agreements.

C. WHEN DO BUSINESSES NEED TO OBTAIN CONSENT TO USE PERSONAL INFORMATION??

The general principle is that personal information can only be used for the purposes for which it was collected and, when the personal information is used internally by a business, only by the authorized employees to whom the information is necessary for the performance of their functions (s. 20 of the Private Sector Act). Law 25 creates an avenue to use implied consent. Section 12 of the Private Sector Act, now reads:

"Unless the person concerned gives his consent, personal information may not be used within the enterprise except for the purposes for which it was collected. Such consent must be given expressly when it concerns sensitive personal information (...)"

Conversely, this implies that when the use does not concern sensitive information, consent to use personal information for purposes that have not been communicated can be implicit rather than explicit. Regardless, to be valid, consent must be clear, free and informed, and given for specific purposes (s. 14 of the Private Sector Act).

At section 12, the Private Sector Act also provides for explicit exceptions where consent does not need to be obtained for businesses to use personal information:

- If it is used for purposes consistent with the purposes for which it was collected, which means that it has a direct and relevant connection with the purposes for which the information was collected;
- If it is clearly used for the benefit of the person concerned;
- When its use is necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures;
- When its use is necessary for the supply or delivery of a product or the provision of a service requested by the person concerned;
- If its use is necessary for study or research purposes or for the production of statistics and if the information is de-identified.

D. WHEN DO BUSINESSES NEED TO OBTAIN CONSENT TO COMMUNICATE PERSONAL INFORMATION?

The Private Sector Act provides that personal information may only be communicated if the person has consented to the sharing of their information (s. 13 of the Private Sector Act). The consent must be express when that information is sensitive.

However, the law also provides two important exceptions to consent for the communication of personal information:

- If the communication of personal information is necessary for carrying out a mandate or performing a contract of enterprise or for services (s. 18.3 of the Private Sector Act). To benefit from this exception, the mandate or contract needs to be made in writing, specify measures required to protect the confidentiality of the personal information communicated, ensure that the information is used only for carrying out the mandate or performing the

contract, and to prohibit the mandatary or person from keeping the information once the mandate or contract has been completed (see section 5(a) – Content of Data Transfer Agreements).

- If the communication of personal information is necessary for concluding a commercial transaction to which a business intends to be a party (s. 18.4 of the Private Sector Act). To benefit from this exception, the business needs to enter an agreement with the other party that will stipulate: that the information will only be used for concluding the commercial transaction; that the information will not be communicated again without the consent of the person concerned; the measures required to protect the confidentiality of the information; and that the information will be destroyed if the commercial transaction is not concluded or if the information is no longer necessary for concluding the commercial transaction.



5 Vendor management

As of September 2023, Law 25 will also have major consequences for businesses doing business in the province that engage in outsourcing or transact with service providers that host or process personal information on their behalf. Service agreements involve transfers, communications, or disclosures of personal information to third parties. The types of agreement vary considerably and includes payment processing, IT services, artificial intelligence (AI) services, business processing outsourcing, and a myriad of different types of cloud computing. Law 25 will add a new layer of regulation on top of the other Canadian and international privacy laws, and other overlapping regulatory regimes that already apply to those transactions.

In addition to requiring businesses to conduct privacy impact assessments prior to communicating any personal information across the provincial border (see section 3(c) – Privacy Impact Assessments) Law 25 will require businesses to review their current templates, agreements, practices and processes. Many service providers' standard forms, customer outsourcing and procurement templates and existing agreements will not comply with Law 25 or will impose consent and transparency burdens on businesses. The risks of not being prepared, or not getting it right, could be high as non-compliance can result in very large administrative monetary penalties, fines, and private rights of action.

A. CONTENT OF DATA TRANSFER AGREEMENTS

Under the Private Sector Act, businesses are exempt from the obligation to obtain consent to disclose personal information to third parties in the context of a pure service agreement. However, the business will still have to have at least the following terms and conditions in its contracts with service providers:

Table 4: Content of Data Transfer Agreements

Security measures	<p>Under section 10 of the Private Sector Act, any business communicating personal information to a service provider for processing must impose security measures to ensure “adequate protection” of the personal information involved. Pursuant to the accountability principle, it is advisable to require the service provider to take security measures to protect personal information 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.</p>
Limiting use of information	<p>Section 12 of the Private Sector Act restricts uses of information provided to a business to those for which consent has been obtained (unless they fall within the list of exceptions – see (unless they fall within the list of exceptions – see the section “4 – <u>Consent</u>”).</p> <p>Contracts with service providers who process personal information should therefore state that the disclosed information is used only for the purposes of carrying out the contract. This limitation will create issues with many standard-form outsourcing contracts which frequently contain terms that permit the service provider to use information for other purposes such as to improve the service provider’s services. It will also create challenges for many AI service agreements which often contain terms permitted customer data to be used for machine learning and related purposes. Given Law 25’s limited exceptions to the consent requirement, businesses must carefully consider what uses service providers can make of personal information provided for processing, unless they are willing to obtain consents from their customers for such uses, or otherwise face the risks of penalties, fines, and class actions should consents not be obtained.</p>
Destruction or anonymization of PI	<p>Contracts with service providers should include a clause that stipulates that information will not be retained when no longer required for the mandate. Section 23 of the Private Sector Act gives businesses the option of either destroying or anonymizing information or using it “for serious and legitimate purposes” when the purposes for which it was collected or used are exhausted.</p>



Security incidents

The Private Sector Act contains provisions related to mandatory confidentiality incident notification requirements that need to be addressed by businesses and their service providers (see section “6 (b) – [Cybersecurity - Incident Management, Incident Log and Breach Reporting Obligations](#)” for more information).

Under section 18.3 of the Private Sector Act, the service provider must notify the business if there has been a breach or an attempted breach of the confidentiality obligations. The requirement to notify disclose “attempted breaches” will also be difficult to implement, as service providers typically do not want to report on “attempted breaches” and will be reluctant to include “attempted breaches” in definitions of reportable “confidentiality incidents”.

To enable businesses to comply with these requirements related to confidentiality incidents, businesses should include service agreement terms that require the service provider to:

- notify the business without “delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated”.
- notify the business of a confidentiality incident of a sufficient degree of seriousness and with sufficient information to enable the business to determine whether the incident presents a risk of serious injury to trigger the notification requirements. The service agreement must address Law 25’s nuances regarding when notifications by the business must be given.
- “take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature” if the service provider “has cause to believe that a confidentiality incident involving personal information the person holds has occurred”.
- “keep a register of confidentiality incidents” and to provide appropriate access to same to enable the business to comply with Law 25 which, at a minimum, must provide that “A copy of the register must be sent to the Commission at its request”. This is similar to the existing Personal Information Protection and Electronic Documents Act (“PIPEDA”) requirement which, even today, some widely used outsourcing providers push back on providing.

Audit rights

The business must have verification (or audit) rights to ensure that the required security measures have been implemented by the service provider.



Other considerations businesses might have with regards to service agreements:

Table 5: Additional Considerations in Data Transfer Agreements

Disclosures that information may be processed outside	Businesses should not forget that, under section 8 of the Private Sector Act, they are required to inform individuals when the information is collected (or subsequently upon request) that the information could be disclosed outside Québec. Individuals must also be informed of the names of the third persons or categories of third persons to whom personal information will be disclosed.
Providing access to information	Law 25 contains obligations on businesses to provide access to information in particular formats (See section “3 (d) iii on Right to data portability ”) and provides individuals a right to correct information if it is inaccurate, incomplete or equivocal (see section “3 (d) i on Right to access and rectification ”). Businesses should keep in mind these obligations in their service agreements.

B. AUTOMATED DECISION-MAKING

Law 25 imposes new obligations on businesses that use personal information to render decisions based exclusively on automated processing. Businesses must inform the individual concerned that the decision was rendered exclusively through automated processing at the time that it informs that same individual of the decision (s. 12.1(2) of the Private Sector Act). Additionally, the individual has the right to request and receive information related to the personal information used to render the decision and the reasons and the principal factors and parameters that led to the decision. The business also must disclose to the individual at their request information pertaining to their right to correct the personal information used to render the decision.

Businesses that use automated decision-making must also put in place a process by which individuals can submit observations to an employee of the business who is able to review the automated decision



6 Biometrics, Cybersecurity, Research and Data Analytics

A. BIOMETRICS

As of September 2023, Law 25 creates new obligations for businesses that work with biometric information through some incremental amendments to sections 44 and 45 of the *Act to Establish a Legal Framework for Information Technology* ("IT Act"). The Government of Québec defines biometrics as any information that can be used to identify someone based on their unique characteristics, including bodily, behavioural, and biological. They provide examples of biometric data such as fingerprints, handshape, facial recognition, and voice recognition.

Businesses that create, use, or obtain a database of biometric information must disclose it to the Commission no later than 60 days after it is brought into service (s. 45 of the IT Act). Additionally, the existence of such a database, irrespective of its state of operation, must be disclosed to the Commission.

Businesses that create, use, or obtain a database of biometric information must disclose it to the Commission no later than 60 days after it is brought into service.

Biometric data is considered sensitive information under Law 25. As a result, any personal information with a biometric character may only be collected by a business if they obtain the express consent of the individual whose biometric information is being collected (s. 44 of the IT Act).

Businesses must also disclose to the Commission the following details about their use of biometric information to verify or confirm the identity of an individual before that individual consents to providing it, irrespective of whether or not a database of that information is ever established:

- the type of biometric data being collected
- the purpose for which it will be used
- security measures in place to protect it
- any third parties it may be shared with
- how long it will be retained and the individual's right to access and rectify it
- alternatives to biometric data use if the individual does not consent to sharing their biometric information.





Businesses must conduct a privacy impact assessment before the collection and use of biometric information (see section 3(c) – [Privacy Impact Assessments](#)). Businesses must provide alternative means of identification if the individual refuses to share their biometric information. They must also limit the collection of biometric information to the minimum required for their purposes, only share it with third parties with the individual's consent or where permitted by law, and destroy biometric information once it is no longer being used to identify the individual, or if the individual withdraws their consent. Individuals retain the right to access and correct their biometric information being held by businesses.

B. CYBERSECURITY - INCIDENT MANAGEMENT, INCIDENT LOG AND BREACH REPORTING OBLIGATIONS

In addition to the broad cybersecurity governance framework (see section “3 – [Governance and Accountability](#)”), Law 25 introduces significant new cyber incident management and reporting requirements for businesses. Businesses now must promptly notify the Commission, as well as any other person whose personal information was affected, of a confidentiality incident that poses a “risk of serious injury”.

Law 25 defines the term “confidentiality incident” as access, use, or communication not authorized by law of personal information as well as a loss or any other breach in the protection of such information. This new definition is coupled with an expanded definition of personal information, with Law 25 adding that personal information includes any information relating to a natural person that can directly or indirectly allow them to be identified.

Law 25 introduces significant new cyber incident management and reporting requirements for businesses

When assessing whether a confidentiality incident poses a risk of serious injury to a person whose personal information is concerned by a confidentiality incident, the business must consider, in particular, the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes.

In addition, Law 25 requires businesses to keep a register of all confidentiality incidents in the manner prescribed by regulation, regardless of whether or not they pose a risk of serious injury.

Law 25 also introduces unique risk mitigation and remediation obligations regardless as to whether or not the confidentiality incident results in a “risk of serious injury” and applies the obligation to any person with cause to believe a confidentiality incident has occurred.

We note that, on December 14, 2022, the *Regulation respecting confidentiality incidents* (the “**Law 25 Regulation**”) was published in the *Gazette officielle du Québec*. The Law 25 Regulation, which came into force on December 29, 2022,

provides businesses with details related to the content of the new notification and record-keeping requirements in the context of confidentiality incidents. Below, we describe the content of these new notifications and record-keeping obligations, comparing and contrasting them with analogous requirements under federal and Alberta law.

i. Existing Requirements under PIPEDA and Alberta PIPA

Similar to the above-mentioned provisions of Law 25, PIPEDA and Alberta's Personal Information Protection Act ("**Alberta PIPA**") require businesses to report any "breach of security safeguards" to the federal or Alberta commissioner, as applicable, and to affected individuals when there is a "real risk of significant harm". Moreover, the content requirements for PIPEDA and Alberta PIPA's breach notification and record-keeping are set out in the Breach of Security Safeguards Regulations ("**PIPEDA Regulation**") and Personal Information Protection Act Regulation ("**Alberta PIPA Regulation**"), respectively.

Law 25's definition of "confidentiality incident" could extend to activities beyond the existing "breach of security safeguards" under PIPEDA or Alberta PIPA. Moreover, the "risk of serious injury" notification standard introduced by Bill 64 differs from PIPEDA and Alberta PIPA's established "real risk of significant harm" standard. Businesses should thus be mindful that this wording could be interpreted in a manner that is more stringent than the PIPEDA and Alberta PIPA standard.

Law 25's definition of "confidentiality incident" could extend to activities beyond the existing "breach of security safeguards" under PIPEDA or Alberta PIPA.

ii. Notice to the Commission

Some of the required information that businesses would need to provide to the Commission under the Draft Law 25 Regulation mirrors obligations found in the PIPEDA Regulation and the Alberta PIPA Regulation. These include:

- the date or time period when the incident occurred or, if unknown, the approximate time period;
- a description of the personal information affected by the incident;
- a description of the circumstances and, if known, the cause of the incident;
- the number of individuals affected, including the number of affected Québec residents;
- the steps taken to reduce the risk of injury;
- the business's contact information; and





- a description of the elements that led the business to conclude that there is a risk of serious injury to the persons concerned, such as the sensitivity of the personal information concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use, and the likelihood that such information will be used for injurious purposes (this obligation is only found in the Alberta PIPA Regulation, although less detailed).

The Law 25 Regulation would also require that businesses provide certain information to the CAI that, while not formally required under the PIPEDA Regulation or Alberta PIPA Regulation, is found in the breach reporting forms recommended by the regulatory authorities. This information includes:

- the date or time period when the body became aware of the incident;
- the date when affected individuals were notified, or the expected time limit for the notification;
- the name of the company;
- the measures aimed at preventing future incidents of the same nature; and
- if applicable, an indication that a privacy commissioner outside of Québec has been notified of the incident.

The Law 25 Regulation would introduce certain disclosure requirements not found under either the PIPEDA Regulation or the Alberta PIPA Regulation. The notice to the Commission must include an explanation if it is impossible to provide a description of the personal information involved.

The Law 25 Regulation would also require that businesses provide certain information to the Commission.



In addition, the Law 25 Regulation would oblige businesses to keep the Commission updated with all additional or new information subsequent to the initial report. The PIPEDA Regulation only provides an optional reporting requirement for any additional information related to the breach. No equivalent provision is found in the Alberta PIPA Regulation.

iii. Notice to the persons concerned

As with the notice to the Commission, the obligations regarding notification to affected individuals is very similar to the PIPEDA and Alberta PIPA regimes. The Law 25 Regulation would require that the notification sent by businesses to individuals affected by the confidentiality incident (where such incident involves a “risk of serious injury”) include the date or time period when the incident occurred or, if unknown, the approximate time period; a description of the personal information affected by the confidentiality incident; the steps taken to reduce the risk of injury; and the business’s contact information. Similar requirements are found in the PIPEDA Regulation and Alberta PIPA Regulation.



In addition, the Law 25 Regulation would require that the notice include a description of the steps that can be taken by the individual to reduce the risk of injury or to mitigate the injury resulting from the incident. A similar obligation is found under the PIPEDA Regulation. Finally, common to all three regimes is the direct notification requirement to the persons concerned should be the primary approach of notification, subject to certain exceptions.

The only unique Québec element with respect to notifying affected individuals is the requirement to include an explanation of why it is impossible, if applicable, to furnish a description of the personal information involved in the confidentiality incident. The same unique Québec requirement is found in the provisions for notification to the Commission.

iv. Record-keeping requirements

The Law 25 Regulation would require that businesses keep in a register a record of all confidentiality incidents for at

least 5 years which would have to minimally include the following information:

- the date or time period when the incident occurred or, if unknown, the approximate time period;
- a description of the personal information affected by the incident;
- a description of the circumstances and, if known, the cause of the incident;
- the number of individuals affected; and
- the steps taken to reduce the risk of injury.

Moreover, the information in the register must be kept up to date.

By contrast, the PIPEDA Regulation requires records to be kept for 24 months and does not specify the content of the record, nor does it require updates. Meanwhile, the Alberta PIPA Regulation does not contain any record-keeping obligation.



C. RESEARCH AND DATA ANALYTICS

Law 25 made various changes to the legislation governing the use of personal information for internal research, bringing Québec's privacy laws more in line with those of other Canadian provinces.

By explicitly allowing the use of de-identified personal information (including sensitive information) without consent, the amendments also introduce significant new plasticity to the regime governing the use of personal information in the context of secondary research and data analytics purposes, such as R&D.

i. Consent exception for research

Law 25 amends the Private Sector Act's section 21 and introduces new sections 21.0.1 and 21.2.2 to modernize the current process for the communication of personal information for research purposes with the goal of simplifying the underlying mechanisms involved.

Under Law 25, businesses may communicate personal information without the consent of the persons concerned to a third party wishing to use the information for study or internal research purposes or for the production of statistics. The information may only be communicated if a privacy impact assessment concludes that:

- the objective of the study or research or of the production of statistics can be achieved only if the information is communicated in a form allowing the persons concerned to be identified;
- it is unreasonable to require the person or body to obtain the consent of the persons concerned the objective of the study or research or of the production of statistics outweighs, with regard to the public interest, the impact of communicating and using the information on the privacy of the persons concerned;
- the personal information is used in such a manner as to ensure confidentiality; and
- only the necessary information is communicated to the third party.

A person who communicates personal information in accordance with section 21 must first enter into an agreement with the person or body to whom or which the information is to be sent that stipulates, among other things, that the information:

- may be made accessible only to persons who need to know it to exercise their functions and who have signed a confidentiality agreement;
- may not be used for purposes other than those specified in the detailed presentation of the research activities;
- may not be matched with any other information file that has not been provided for in the detailed presentation of the research activities; and
- may not be communicated, published or otherwise distributed in a form allowing the persons concerned to be identified.

The agreement must be sent to the Commission and comes into force 30 days after it is received by the Commission.

ii. Consent exception for data analytics

As of September 2023, Law 25 will amend section 12 of the Private Sector Act to enable businesses to use personal information that was initially collected for one purpose, without consent, to use it within the same business for purposes consistent with the purposes for which it was collected (s. 12 para. 2(1)) and study or research or for the production of statistics, if the information is de-identified (s. 12 para. 2(3)). Law 25 considers information to be de-identified if it no longer allows the person concerned to be directly identified. Any business using de-identified information must take reasonable measures to limit the risk of someone identifying a natural person using de-identified information.

We note that such internal research or data analytics initiatives would call for a privacy impact assessment if it is related to a “project of acquisition, development and redesign of an information system project or electronic service delivery” (s. 3.3 of the Private Sector Act).





7 Privacy by Design

Law 25 furthers the principle of privacy by design. First, it requires that all technological products and services must have their privacy settings set to the highest level of privacy by default.

Businesses must ensure that any product or service they offer that has different levels of privacy settings has those settings set to the highest level of privacy, confidentiality, and data protection by default. Technology devices and services must automatically be set to the highest level of privacy setting. Reaching the highest level of privacy for a product or service must require no intervention from the consumer, who must opt in to any privacy setting that is lower than the highest. Relevant technologies could include, for example websites, social networking accounts, mobile applications, and connected devices. This rule has a specific exception for browser cookies. Browser cookies are exempt from the privacy by default requirement.

Second, Law 25 create new obligations for businesses that use profiling technology. Profiling technology is technology that is used to collect personal information that allows that person to be identified, located, or profiled. Law 25 specifically defines profiling as “the collection and use of personal information to assess certain characteristics of [an individual], in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour” (s. 8.1 of the Private Sector Act).

Businesses that use this technology must inform the individuals whose information is being collected that such technology is being used. They must also inform the individual of “the means available to activate the functions that allow a person to be identified, located or profiled” (s. 8.1 of the Private Sector Act). Although this requirement is presented as a transparency obligation, it implies more broadly that the identification, localization or profiling functions of a technology must be inactive by default.

FOR MORE INFORMATION, PLEASE CONTACT:



Charles Morgan
Co-Leader,
Cyber/Data Group, Partner
cmorgan@mccarthy.ca
514-397-4230
MONTREAL



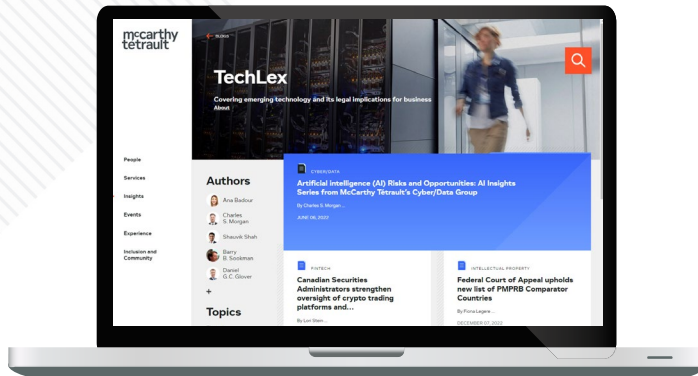
Eugen Miscoi
Associate,
Cyber/Data Group
emiscoi@mccarthy.ca
514-865-2393
MONTREAL



Dan Glover
Co-Leader,
Cyber/Data Group, Partner
dglover@mccarthy.ca
416-601-806
TORONTO

Please let us know if you have any additional questions related to any of the points discussed above. This toolkit may be updated from time to time, as additional regulatory developments and relevant guidance published by the Commission and other stakeholders becomes available.





VISIT OUR TECHLEX BLOG:

<https://www.mccarthy.ca/en/insights/blogs/techlex>

FOLLOW US ON TWITTER:

[@McCarthy_ca](https://twitter.com/McCarthy_ca)

About our Cyber/Data Group

Combining a national presence and cross-practice approach across industries, the Cyber/Data Group offers a 360° view of data and cyber strategy to deliver legal and business solutions that mitigate risks and unlock value-generating potential. Our integrated multidisciplinary team works seamlessly across borders, advising global businesses through some of the largest cybersecurity incidents and regulatory investigations in Canadian history and is changing the state of Canadian privacy, cybersecurity and data law like no other firm.

McCarthy Tétrault LLP is a premier full-service Canadian law firm advising on large and complex transactions and disputes for domestic and international clients. The firm has offices in every major business center in Canada, and in New York and London. The firm's industry-based team approach and depth of practice expertise helps our clients achieve exceptional commercial results.

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5

CALGARY

Suite 4000, 421 7th Avenue
Calgary AB T2P 4K9

TORONTO

Suite 5300, TD Bank Tower, Box 48
66 Wellington Street West
Toronto ON M5K 1E6

MONTREAL

Suite MZ 400
1000 De La Gauchetière Street West
Montréal QC H3B 0A2

QUÉBEC CITY

500, Grande Allée Est, 9e étage
Québec QC G1R 2J7

NEW YORK

55 West 46th Street, Suite 2804
New York, New York 10036
United States

LONDON

1 Angel Court, 18th Floor
London EC2R 7HJ
United Kingdom