Borden Ladner Gervais

Québec Privacy Law Reform:
Compliance Guide for Organizations

October 2022

Québec Privacy Law Reform: Compliance Guide for Organizations

This Guide is intended to help organizations prepare for the coming into force of the new requirements introduced to the *Act respecting the protection of personal information in the private sector* ("**Private Sector Act**") following the adoption of Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* ("**Bill 64**"*). While similar efforts are underway in a number of Canadian jurisdictions, Québec is officially the first jurisdiction in Canada to update its privacy legislation, bringing it closer in line with the landmark European Union's *General Data Protection Regulation* ("**GDPR**").

The Guide is divided into different topics that reflect the key changes introduced by Bill 64 to Québec's private sector data protection framework. It is designed for any person who collects, holds, uses or communicates personal information in the course of carrying on an enterprise within the meaning of section 1525 of the *Civil Code of Québec* ("**Civil Code**") (in the present Guide, an **organization**").

Steps to Compliance

Under each topic, we have outlined some suggested steps that organizations could consider to get a head start in terms of compliance and prepare for the coming into force of the new provisions.

Legal Uncertainties

Furthermore, given that Bill 64 introduces a number of new concepts into Québec's data protection framework, some provisions are likely to raise their own challenges and require further interpretation. We have therefore identified areas where businesses should pay particular attention using the **! symbol**.

* This abbreviation is consistent with the usual practice of referring to a particular Act by the number of the bill from which it originated (e.g. Bill 101, Bill 21, Bill 96, etc.). However, some use the term "Act 25" in reference to the chapter number (c. 25) of the *Act to modernize legislative provisions respecting the protection of personal information* in the 2021 Annual Statutes of Québec, which corresponds to the order of the sanction of that Act in the year 2021.

Table of Contents

Coming into force

First, it is important to clarify the timeframe that organizations have to adjust their practices before Bill 64's new requirements come into force. Thus, subject to some exceptions, the amendments to the Private Sector Act will come into force on **September 22, 2023**, namely two years after the date of assent of Bill 64. However, some provisions came into force on September 22, 2022 (for instance, the role of the Privacy Officer and mandatory breach reporting, see new sections 3.1 and 3.5 to 3.8). Note that the right to data portability (s. 27 para. 3) is the only provision of Bill 64 that will come into force on September 22, 2024. We prepared the following table to summarize the coming into force dates for the main amendments introduced by Bill 64.

Bill 64 Section(s)	Requirement	Coming into force	Link in this guide
3.1	Designation of a person in charge of the protection of personal information	**September 2022**	Section 2.1
3.2	Governance policies and practices regarding personal information	**September 2023**	Section 2.2
3.3 and 3.4	Privacy impact assessments	**September 2023**	Section 2.3
3.5 to 3.8	Mandatory reporting of confidentiality incidents	**September 2022**	Section 7.2
8 and 8.2	Transparency and privacy notices	**September 2023**	Section 3.1
8.1	Identification, geolocation tracking and profiling technologies	**September 2023**	Section 3.2
8.3, 12 and 14	New consent requirements	**September 2023**	Section 3
9.1	Privacy by default	**September 2023**	Section 2.4
12	New consent exceptions	**September 2023**	Section 3.3
12.1	Automated decision making	**September 2023**	Section 4.3 and 5.3
17	Transfers of personal information outside Québec	**September 2023**	Section 6.2

Bill 64 Section(s)	Requirement	Coming into force	Link in this guide
18.3	Outsourcing personal information	**September 2023**	Section 6.1
18.4	Communication of personal information for concluding a commercial transaction	**September 2022**	Section 3.3
21 to 21.0.2	Communication of personal information for research purposes	**September 2022**	Section 4.1
23	Retention and destruction of personal information	**September 2023**	Section 7.1
27	Right to data portability	**September 2024**	Section 5.2
28.1	Right to be forgotten	**September 2023**	Section 5.1
90.1 to 93.1	New enforcement mechanisms	**September 2023**	Section 1
44 and 45	Amendments to the biometrics provisions of QC IT Act	**September 2022**	Section 7.3

1. New enforcement mechanisms

Effective September 22, 2023

Bill 64 provides three different types of mechanisms to enforce compliance under the Private Sector Act: (1) administrative monetary penalties, (2) penal offences, and (3) a private right of action.

Administrative Monetary Penalties (ss. 90.1 to 90.17). Bill 64 introduces an entirely new administrative monetary penalty ("**AMP**") regime administered by Québec's privacy regulator, the Commission d'accès à l'information ("**CAI**"). Under these new provisions (sections 90.1 to 90.17), a "person designated by the Commission, but who is not a member of any of its divisions" will have the power to impose AMPs on organizations that contravene the law (see the table below for specific offences) of up to $10,000,000 or 2% of worldwide turnover. Despite the significance of this new enforcement mechanism, the status of the particular person in charge of imposing AMPs remains unknown. This being said, Bill 64 provides that the CAI must publish a general framework for the application of AMPs, which specifies, among other things, the purposes of the AMPs and the criteria used to decide to impose such penalties and to determine its amount (art. 90.2). This framework could be similar to the one developed by the Ministère de l'Environnement et de la Lutte contre les changements climatiques (available in French only) for the application of the AMP regime under provincial environmental legislation.

Penal offences (ss. 91 to 93). Bill 64 creates several new offences under the Private Sector Act (see table below for specific offences) under which the CAI may institute penal proceedings. These infractions may be sanctioned by a fine of up to $25,000,000 or 4% of worldwide turnover, which is imposed by the Court of Québec.

Punitive Damages (s. 93.1). Bill 64 recognizes the possibility for individuals to claim punitive damages when an unlawful infringement of a right conferred by the Private Sector Act or by articles 35 to 40 of the Civil Code causes an injury, provided the infringement is intentional or results from gross negligence. Section 93.1, which will come into force on September 22, 2023, is therefore a new provision for the award of punitive damages within the meaning of article 1621 of the Civil Code.

The following tables provide a summary of the new enforcement mechanisms introduced by Bill 64 into the Private Sector Act.

1.1. Violation

	Penal offence	AMP	Punitive damages
Collection, use, disclosure, retention or destruction of personal information in contravention of the Private Sector Act	6	6	6
Failure to inform the individuals in accordance with sections 7 and 8 at the time of collection		6	6
Failure to take appropriate security measures necessary to ensure the protection of personal information pursuant to section 10	6	6	6
Failure to notify the CAI or the individuals concerned of a confidentiality incident that presents a risk of serious injury	6	6	6
Failure to inform the individual affected by a decision based on an automated processing of personal information or provide an opportunity submit observations		6	6
Identify or attempt to identify an individual using de-identified or anonymized information without the authorization of the organization who holds the information	6		6
Impede the progress of an investigation, an inspection or the hearing of an application by the CAI	6		
Take a reprisal against an individual on the ground that the individual has, in good faith, filed a complaint with the CAI or cooperated in an investigation	6		6
Failure to comply with a request for production of documents issued by CAI within the specified time	6		
Failure to comply with an order from the CAI	6		

1.2. Procedural aspects

	Penal offence	AMP	Punitive damages
Limitation period	5 years	2 years	3 years
Prior Notice of Non-Compliance	Optional*	Yes	No
Option to enter into an undertaking with the CAI	No	Yes	No
Penalty imposed by	Court of Québec	A person designated by the CAI	Court of Québec or Superior Court (depending on the amount of the claim)
Application for review	No	Yes	No
Right of appeal or contestation	Yes – Superior Court	Yes – Court of Québec	With the permission of a judge of the Court of Appeal (if the value of the claim is less than $60,000)

* The new section 90.2 provides that a notice of non-compliance must mention the fact that the violation identified by the CAI could result in an AMP or a penal sanction. However, the obligation to send a notice of non-compliance to the offending organization only arises before imposing an AMP (s. 90.4). Thus, it is not readily clear whether the institution of penal proceedings by the CAI will necessarily be preceded by a notice of non-compliance providing a deadline to remedy the violation. That said, the new section 92 makes it clear that the CAI's penal proceeding is subject to the provisions of Québec's *Code of Penal Procedure*.

1.3. Penalties

Penal offence	AMP	Punitive damages
Maximum Penalty		
$25,000,000 or 4% of worldwide turnover for the preceding year	$10,000,000 or 2% of worldwide turnover for the preceding year	Amount of punitive damages awarded (at least $1000)
Determining Factors		
• The nature, seriousness, repetitiveness, and duration of the offence • The sensitivity of the personal information involved • Whether the offender acted intentionally or with recklessness or negligence • The foreseeability of the offence or the failure to act on recommendations or warnings to prevent it • The offender's attempts to conceal the offence or failure to mitigate its consequences • The failure of the offender to take reasonable steps to prevent the commission of the offence • Whether the offender, in committing the offence or in failing to take steps to prevent its commission, increased his or her income or reduced his or her expenses or intended to do so • The number of individuals affected by the offence and the risk of harm to those individuals	• The nature, seriousness, repetitiveness and duration of the violation • The sensitivity of the personal information involved • The number of individuals affected by the violation and the risk of harm to those individuals • The measures taken by the organization to remedy the failure or mitigate its consequences • The degree of cooperation provided to the CAI to remedy the failure or mitigate its consequences • The compensation offered by organization, as restitution, to every individual affected • The organization's ability to pay, given such considerations as to its assets, turnover and revenues	Based on case law.

2. Accountability and governance

Bill 64 formally recognizes that every organization is responsible for the protection of personal information it holds (s. 3.1 para. 1). This principle gives rise to a number of accountability and data governance obligations, some of which came into force in September 2022.

2.1. Privacy Officer

Effective September 22, 2022

Designation. Bill 64 provides that, by default, the person with the highest authority within the organization (e.g., its CEO) acts as the "**Privacy Officer**" and is responsible for ensuring compliance with the Private Sector Act (s. 3.1 para. 2). However, this role of "Privacy Officer" may be delegated in writing, in whole or in part, to any person (s. 3.1 para. 2). This can be a member of the personnel of the organization or a third party. In any event, the organization must ensure that the title and contact details of its Privacy Officer are available on its website (s. 3.1 para. 3).

Duties. At a minimum, the Privacy Officer is responsible for carrying out the following tasks:

- Approve governance policies and practices regarding the protection of personal information that the organization must establish and implement (s. 3.2 para. 1). See section 2.2 below for more details on these policies and practices.
- Participate in the conduct of Privacy Impact Assessments ("PIAs") involving certain information systems or electronic service delivery systems (s. 3.3 para. 2) and suggest measures to ensure the protection of personal information processed in connection with such systems (s. 3.4). See section 2.3 below for more details on PIAs.
- Record any communication (without consent) to another organization or public body that may reduce the risk of injury resulting from a confidentiality incident (s. 3.5 para. 2) and advise the organization in the assessment of the risk of injury resulting from a confidentiality incident (s. 3.7). See section 7.2 for more details on confidentiality incidents.
- Receive and respond to access and rectification requests as well as requests related to data portability and the right to be forgotten (s. 32, 34, 35). See section 5 for more details on new individual rights.

Qualifications. Bill 64 does not explicitly mandate the Privacy Officer to be located in Québec, have specific knowledge of Québec law or have a knowledge of French. The Québec entity of a business group with international operations could therefore potentially delegate the role of Privacy Officer to an individual who performs a similar role at the national (e.g. Canada), regional (e.g. North America) or global level.

Differences with the GDPR. It is interesting to note some differences between the role of Privacy Officer and the role of Data Protection Officer under the GDPR (see Articles 37 and 38 of the GDPR):

- No requirement to allocate resources to the Privacy Officer under Bill 64.
- No prohibition on the organization giving instructions to the Privacy Officer.
- No prohibition on the use of retaliatory action against the Privacy Officer (although anyone who files a complaint or cooperates with a CAI investigation is protected from retaliation.)
- No requirement to disclose the contact information of the Privacy Officer to the CAI (although the CAI has broad powers to request such information; this information must also be made available on the organization's website).

Steps to compliance

1. **Determine the qualifications required to fulfill the role of Privacy Officer.** Organizations should determine whether they have the necessary expertise in-house, whether they wish to hire someone to perform the role, or whether they wish to outsource the role.
2. **Establish a description of the roles and responsibilities of the Privacy Officer.** This description should take into account the requirements of Bill 64 and the reality of the organization.
3. **Designate an individual as the Privacy Officer in writing. Provide a training program for the Privacy Officer.** Provide a training program for the Privacy Officer.
4. **Publish the contact information of the Privacy Officer on the organization's website.**

2.2. Governance policies and practices regarding the protection of personal information

Effective September 22, 2023

Bill 64 formally recognizes the duty of organizations to establish and implement governance policies and practices relating to the protection of personal information (s. 3.2 para. 1). These policies and practices must, among other things, provide a framework applicable to:

- the retention and destruction of personal information;
- the roles and responsibilities of the personnel throughout the life cycle of the information; and
- a process for dealing with complaints regarding the protection of the information

In addition, an organization is required to publish "detailed information about these policies and practices" on its website in clear and simple terms (s. 3.2 para. 2). This is a unique requirement in Canada and the level of detail that will be expected from an organization is not expressly defined. There appears to be no prohibition against including this information in the organization's privacy policy.

Organizations may want to consider incorporating this information into a new section of their website dedicated to privacy. An increasing number of organizations are creating this type of section (e.g., a "Privacy Center"), conveniently centralizing relevant information about the organization's privacy program. This may include, for example, a commitment to the protection of personal information, a privacy policy, frequently asked questions on privacy matters, information on the organization's security certifications (e.g. ISO 27001 or SOC 2, etc.), just to name a few examples.

Steps to compliance

1. **Conduct an inventory of the policies and procedures in place to protect personal information throughout its life cycle.**
2. **Conduct a data mapping exercise to document the organization's personal information management practices.** This exercise will be useful in developing the policies outlined below.
3. **Update or establish the following policies and procedures, which should establish the roles and responsibilities of the organization's employees throughout the life cycle of the information. Organizations should implement the following policies (or incorporate them into an "internal privacy framework"):**
    - Policy setting out the general principles relating to the collection, use and disclosure of personal information.
    - Data retention policy and retention schedule.
    - Procedures for the destruction of personal information and anonymization, if applicable.
    - Policy and procedures for receiving and processing complaints and requests from individuals wishing to exercise their rights.
    - Policies and procedures relating to data security.
    - Policy for handling confidentiality incidents and incident response plan.
    - Policies specific to the organization's activities, for example: policy on the use of surveillance cameras, policy on the use of biometric systems, policy on the use of personal information for research and artificial intelligence, etc.
4. **Develop a privacy training program for employees who handle or have access to personal information.**
5. **Have these policies and practices approved by the Privacy Officer.**
6. **Publish detailed information about these policies and practices on the organization's website (e.g., by including it in its privacy policy) or by creating a separate section on its website.**

2.3. Privacy Impact Assessments ("PIAs")

Effective September 22, 2023

Requirement to conduct a PIA. Organizations will be required to conduct a PIA prior to the acquisition, development or redesign of an information system or electronic service delivery project involving the collection, use, disclosure, retention or destruction of personal information (s. 3.3 para. 1). A PIA is a preventative process that seeks to better protect personal information and ensure that the privacy interests of individuals are taken into account at the outset of a project involving the processing of personal information. The nature, scope and content of the PIA may vary depending on the context but generally include (i) a description of the project and its data processing operations (e.g., types of information collected, used or disclosed, the purpose(s) for which information is processed, the period for which information is retained, the parties involved in the processing, etc.); (ii) an evaluation of the project's compliance with key privacy principles and requirements (e.g., transparency, consent, accountability, data security, etc.); and, (iii) the identification and evaluation of the privacy risks resulting from the project. This information will then serve as the basis for developing, documenting and implementing a strategy for mitigating the risks previously identified and monitoring compliance. This process is most effective when it is carried out in the early stages of a project's design or development, as it allows the organization to manage privacy risks before they arise and to implement privacy-enhancing features.

Examples of projects covered by the requirement. The CAI has published a guide on PIAs (Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée, available in French only), which was updated in March 2021. This guide does not explicitly reflect the requirements of Bill 64, but the CAI has indicated that it will update and significantly revise this guide in light of Bill 64. In this guide, the CAI recommends that a PIA be conducted for any project involving personal information. While this is a much broader requirement than the one set out in Bill 64, it is still interesting to highlight some of the projects this may cover:

- Developing a new information system or a personalization feature for a product or service;
- Searching for new customers, exploring new markets;
- Using an algorithm or an artificial intelligence system;
- Installing a video surveillance system;
- Comparing different versions of databases or files;
- Acquiring or merging organizations;
- Using fingerprints, geolocation, facial recognition, connected objects, smart city sensors, etc.

Not retroactive. The requirement to conduct a PIA is not retroactive. Thus, organizations will not have to assess existing systems when the new section 3.3 comes into force. However, a substantial update to an existing system (e.g., a document management platform) could be considered a "redesign" and will therefore require a PIA.

Format and scope of the PIA. The PIA must be "proportionate to the sensitivity of the information concerned, the purpose for which it is to be used, the quantity and distribution of the information and the medium on which it is stored" (s. 3.3 para. 4). It should be noted that the same criteria are used to determine the types of security measures that an organization must implement to protect the personal information it holds (s. 10). This proportionality requirement is ostensibly intended to ensure that the scope of the PIA is adapted to the risk of harm and impact of the project on an individual's privacy interests. A project involving minimal personal information, which is not very sensitive, would not require the same type of PIA as the implementation of a biometric system involving a large number of individuals, for example. Note that the CAI's guide on PIAs provides useful tools for organizations that want to become familiar with the process.

Data portability. In addition, organizations will need to ensure that new projects and systems are able to accommodate data portability, i.e., the ability for individuals to receive their personal information in a structured and commonly used technological format (s. 3.3 para. 3). See section 5.3 for more details on the right to data portability.

Steps to compliance

1. **Develop an internal PIA procedure.** The procedure should, among other things:
    - Define clear thresholds that trigger the requirement to conduct a PIA. For example, the organization could develop a matrix to assess the need for a PIA based on the organization's activities.
    - Establish a process to ensure that projects requiring a PIA are identified in the early stages of their development.
2. **Share the procedure within the organization.**
    - Organizations can designate "champions" in the various departments that may initiate such projects (marketing, IT, business intelligence, procurement).
    - These individuals, who are responsible for their respective department, should inform the Privacy Officer at the outset of a project requiring a PIA.
3. **Develop a PIA template.**
    - The template should be in a user-friendly format so that operations staff without advanced privacy knowledge can complete a first draft.
    - Train appropriate staff on how to complete a PIA.

2.4. Privacy settings and privacy by default

Effective September 22, 2023

Highest level of confidentiality. Bill 64 provides that an organization that collects personal information when offering to the public a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the individual (s. 9.1 para. 1). However, browser cookies are expressly exempt from this requirement (art. 9.1 para. 2). Based on the wording of the provision, we understand that it also does not apply to a product or service intended for employees of an organization (e.g., intranet, mobile application for employees, etc.). We should also note that this new requirement does not provide any qualifiers for determining what will be considered the "highest level of confidentiality" in a given context. It is therefore likely to cause interpretive challenges for organizations.

Privacy by design. This requirement appears to be inspired by the notion of "privacy by design" that is found, most notably, in Article 25 of the GDPR. This notion seeks to ensure that the individuals' right to privacy is considered and respected at every stage of the development process of an initiative, and makes all stakeholders accountable for ensuring that a specific product or service protects privacy. The obligation under Bill 64, however, appears to be much narrower in scope, as it only concerns the privacy parameters of certain technological products or services and not the entire development cycle of such products or services.

Cookies and Other Technological Functions. The interaction of the new section 9.1 with section 8.1 (see section 3.2) with respect to cookies raises confusion. While the legislator specifically excluded cookies from the scope of section 9.1, it did not exclude them from the scope of section 8.1. This latter provision applies to the collection of personal information by any technological means that include functions that allow an individual to be profiled, located or identified. In this case, an organization must inform individuals of the means available to activate these functions. This implies some positive action on the part of the individual to signify their intention to activate a specific function. Moreover, according to legislative debates and comments issued by the CAI, this provision could require an organization to deactivate these functions by default (see section 3.2). For these reasons, certain types of cookies may be subject to the deactivation by default requirement of section 8.1 if they collect personal information for prescribed functions.

Steps to compliance

1. **Prepare an inventory of the technological products or services offered to the public that collect personal information and that have privacy parameters.**
2. **Prepare an inventory of all technologies used to collect personal information and determine whether they include functions that allow an individual to be profiled, located or identified.**
3. **Assess whether these privacy settings or technological functions need to be adjusted to comply with new privacy by default requirements. This may include adjusting certain privacy settings to provide the highest level of confidentiality by default and implementing new processes to request user activation for specific functions.**

3. Transparency and consent

Bill 64 clarifies the applicable transparency and consent rules in the Private Sector Act.

3.1. Transparency and obligation to inform prior to consent

Effective September 22, 2023

Clear and simple language. In terms of transparency, organizations have an obligation to provide certain information in "clear and simple language", regardless of the means used to collect the information (s. 8 para. 4).

Obligation of transparency. This obligation of transparency arises at the time of collection (and subsequently on request) or, in some cases, only on request and, where applicable, upon the use of certain technologies:

- **At the time of collection.** The organization that collects personal information from an individual must, when the information is collected and subsequently on request, inform the individual of: (i) the purposes for which the information is collected; (ii) of the means by which the information is collected; (iii) the rights of access and rectification provided by law; (iv) their right to withdraw consent to the communication or use of the information collected; and if applicable: (v) of the name of the third person for whom the information is being collected; (vi) the names of the third persons or categories of third persons to whom it is necessary to communicate the information for the purposes for which it was collected; and (vii) the possibility that the information could be communicated outside Québec (s. 8 para. 1 and 2).
- **On request.** An organization must also inform, on request, the individual of: (i) the personal information collected from them, (ii) the categories of employees who have access to the information within the organization, (iii) the duration of the period of time the information will be kept; and (iv) the contact information of the Privacy Officer (s. 8 para. 3). When collecting information from another organization, an organization must, at the request of the individual, inform them of the source of the information (s. 7), unless this information is part of an investigative file established for the purpose of preventing, detecting or repressing a crime or an offence under the law.
- **Identification, localization and profiling technology.** An organization that collects personal information using technology that includes functions that allow the individual to be identified, located or profiled must inform the individual of the use of such technology and the means of activating these functions (s. 8.1 para. 1 (1) and (2)). The notion of "profiling" is broad and refers to the collection and use of personal information to "assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behaviour" (s. 8.1 para. 2). As such, this new requirement may apply to various technologies as well as in different settings (e.g., employee monitoring tools, cookies and similar technologies used for targeted advertising, etc.).

The interpretation of section 8.1 gives rise to certain difficulties, as it is not clear whether this provision is simply an extension of the transparency obligation under section 8 of the Private Sector Act or whether it is a formal, distinct restriction on the use of localization, identification and profiling technologies. When discussing this new provision during a parliamentary committee, Éric Caire, the Minister responsible for Access to Information and the Protection of Personal Information, indicated this provision introduced an explicit consent (opt-in) requirement for the collection of personal information using technologies with identification, localization or profiling functions. In addition, the CAI, on its website (in French only), mentions that these technologies cannot be activated by default; that it will be up to the person concerned to activate them if he or she so wishes. In other words, the individual must take a positive action to signify their intention to active a specific function. Yet, we note that the wording of section 8.1 only speaks of an obligation to "inform" individuals of the means available to activate these functions, without specifying that these means must in fact exist or that the functions themselves must be systematically disabled. In any case, in light of the CAI's comments, it is prudent to consider reviewing the use of certain technologies to profile, locate or identify individuals and, if necessary, implementing new processes to request user activation for specific functions. See section 2.4. for details on the privacy by default requirements.

- **Collecting through technological means.** An organization that collects personal information through technological means must publish a privacy notice in clear and simple language on the organization's website and disseminate it by any appropriate means that will reach the individuals concerned (s. 8.2). The expression "any appropriate means" is likely meant to encourage an organization to inform individuals of its information handling practices using means that are convenient and easily accessible. An organization has the same transparency obligations (as detailed in s. 8.2) if its practice and/or policy is changed. On the issue of consent, the Office of the Privacy Commissioner ("**OPC**") published a few years ago Guidelines for obtaining meaningful consent in which it provides valuable recommendations that may be relevant to consider when obtaining consent under Bill 64, including, for example, emphasizing certain key elements, allowing individuals to control the level of detail they get (i.e. layered notices), being innovative and creative (e.g., implementing "Just-in-time" notices or other interactive tools) and making consent a dynamic and ongoing process (with guidance on how to manage updates and material changes made to privacy notices).

Automated decision-making. Bill 64 also introduces transparency requirements for an organization using personal information to render a decision based exclusively on automated processing of such information (s. 12.1). See sections 4.3 and 5.3. for details on these requirements.

Steps to compliance

1. **Review and update privacy notices (both those for clients and employees) and consent forms and processes for obtaining consent.** Ensure that the following elements are included in simple and clear terms:
    - Purposes for and means by which the personal information is collected.
    - Rights of access, rectification, and to withdraw consent.
    - Name of the third person for whom the information is being collected (if applicable).
    - Categories of service providers (if applicable).
    - Communication of information outside of Québec (if applicable).
2. **Develop and implement a procedure to respond to the following questions and requests for information (whether from clients or employees):**
    - Personal information collected by the organization from the individual.
    - Categories of employees who may have access to this personal information.
    - Retention period applicable to information collected from the individual.
    - Contact information of the Privacy Officer.
    - Source of the information (if collected from a third party), unless the information was collected in connection with an inquiry to prevent, detect or repress a crime or statutory offence.
3. **Prepare an inventory of technologies that collect personal information (from clients and employees) and determine whether they include functions that allow an individual to be profiled, located or identified. Where applicable, for each function:**
    - Consider whether there are adequate processes in place to inform individuals, at the time of collection, of the use of the technology and the means to activate the function. If appropriate, consider implementing new processes to request user activation.
4. **Determine whether personal information (of clients or employees) is collected through technological means. Where applicable :**
    - Prepare the inventory of these technological means.
    - Publish a privacy policy/notice (in clear and simple language) on the organization's website detailing these collections through technological means.
    - Disseminate the privacy policy through any appropriate means to reach the individuals concerned by the collection of personal information through technological means.
    - Implement a procedure to update the privacy notice to ensure that it accurately reflects the organization's practices and that individuals are adequately informed of any such changes.

3.2. Consent requirements: Form, validity and minors

Effective September 22, 2023

Bill 64 provides certain details regarding the form of consent, which may vary depending on the sensitivity of the information; the criteria that must be fulfilled in order to ensure the validity of the consent; and the requirements for obtaining consent from minors.

Form of consent. With respect to the form of consent, Bill 64 recognizes that an organization may rely on implied consent to process personal information in accordance with the purposes set out in its privacy policy/privacy notice (s. 8.3). That being said, Bill 64 also states that personal information may only be used within the organization for the purposes for which it was collected, and may not be communicated to a third party, except with the consent of the individual or as provided for in the Private Sector Act. This consent must be expressly given when sensitive personal information is involved (s. 12 and s. 13). However, it is not clear whether express consent is required when collecting sensitive personal information from an individual for certain purposes specified at the time of collection, since no distinction is made between sensitive and non-sensitive personal information in section 8.3. Sensitive information is defined as information that, due to its nature, including medical, biometric or otherwise intimate information, or the context of its use or communication, entails a high level of reasonable expectation of privacy (s. 12 para. 4 (2)).

Validity of consent. Bill 64 specifies that valid consent must be manifest, free, informed and given for specific purposes, and be requested for each of those purposes in clear and simple language (s. 14 para. 1). In addition, when a request for consent is made in writing, the organization must ensure that the request is presented separately from any other information communicated to the individual. This may prohibit the bundling of the request for consent for specified processing activities with information about other matters, such as the terms of use of the organization's services. On request, the organization should assist the individual in understanding the scope of the consent sought.

Consent of minors. The consent of a minor under 14 years of age is given by the holder of parental authority or by the tutor (s. 4.1 and 14 para. 2) and the consent of a minor 14 years of age or older may be given by the minor, by the holder of parental authority or by the tutor.

Steps to compliance

1. **Prepare an inventory of personal information collected, used and communicated by the organization** (clients and employees) to determine:
   - Those of a sensitive nature.
   - Those belonging to minors.
   - Those excluded from the scope of the law (i.e. business contact information).
2. **Prepare an inventory of consent forms** or other documents used to obtain consent from individuals (clients or employees) and review them to ensure that :
   - Any consent obtained is clear, free, and informed.
   - Any consent obtained is given for specific purposes in simple and clear language.
   - If the consent is requested in writing, the request is presented separately from any other information provided to the individual.
   - The consent of a minor under 14 years of age is obtained by the holder of parental authority or by the tutor.
   - The consent of a minor 14 years of age or older is obtained by the minor, the holder of parental authority or by the tutor.
3. **Implement a procedure to ensure that on request of an individual** (clients and employees):
   - The organization has a process in place to assist them in understanding the scope of the consent being sought.
4. **Update the organization's classification policy** (or other relevant document) in order to reflect:
   - Information that is sensitive and that belongs to minors.

3.3. Exceptions to the consent requirement

Effective September 22, 2023

except for disclosure (i) in the context of a commercial transaction and (ii) for study, research or statistical purposes (September 22, 2022)

Bill 64 excludes certain information from the scope of the Private Sector Act and introduces new exceptions to the requirement to obtain consent for certain uses or communications of personal information.

Business contact information. Bill 64 excludes "personal information concerning the performance of duties within an organization by the person concerned" from the scope of divisions II and III of the Private Sector Act (i.e., notice and consent requirements). This includes "the person's name, title and duties, as well as the address, email address and telephone number of the person's place of work" (s. 1 para. 5). This exclusion is similar to the one found in the *Personal Information Protection Act* ("**PIPA**") of British Columbia. It is also

broader than the equivalent exemptions found in the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and the *Personal Information Protection Act* ("**PIPA**") of Alberta, as these are generally limited to business contact information used for the sole purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession. While this exemption may be useful to some organizations that wish to use this type of information without consent, they must keep in mind that the use of electronic addresses, such as work email addresses, to send commercial messages remains subject to requirements under Canada's anti-spam legislation.

Use without consent. Under Bill 64, personal information may be used for a purpose other than those for which it was originally collected, without the consent of the individual concerned, in the following situations:

- **Legitimate business purposes.** When its use is necessary for the supply or delivery of a product or the provision of a service requested by the individual (s. 12 para. 2 (2.2)) or necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures (s. 12 para. 2 (2.1)).
- **Interest of the individual.** When it is clearly used for the benefit of the individual (s. 12 para. 2 (2)).
- **Research, data analytics and AI.** When its use is for purposes consistent with those for which it was collected (s. 12 para. 2 (1)) or that its use is necessary for study or research purposes or for the production of statistics and if the information is de-identified (s. 12 para. 3). See section 4.2 for details on this exception and the definitions of "consistent purposes" and "de-identified" information.

Communication without consent. Under Bill 64, personal information may be communicated without consent in the following situations:

- **Outsourcing context.** When the communication is necessary for carrying out a mandate or performing a contract of enterprise or for services and protective measures are in place to protect personal information (s. 18.3). See section 6.1 for details on this exception.
- **Research, data analytics and AI.** When the communication is made to a person or body wishing to use the personal information for study or research purposes or for the production of statistics and that the protective measures provided for in the law are in place (s. 21 to 21.0.2). We note that this exception is not subject to the requirement that the information be de-identified (as is the case for the use of personal information for study or research purposes or for the production of statistics internal to the organization) although a specific framework applies for these types of research projects. See section 4.1 for details on this exception.
- **Commercial transaction.** When the communication is necessary for the conclusion of a commercial transaction (i.e. the disposition or lease of all or part of a business or its assets, a change in its legal structure by amalgamation or otherwise, the obtaining of a loan or other form of financing, or a security interest), if an agreement is reached with the other party, stipulating that the latter undertakes: (i) to use the information only for the purpose of completing the commercial transaction; (ii) not to communicate the information without the individual's consent unless otherwise authorized by law; (iii) to take the necessary measures to ensure the protection of the confidentiality of the information; and (iv) to destroy the information if the commercial transaction

is not completed or if its use is no longer necessary (s. 18.4). When the commercial transaction is completed and the other party wishes to continue to use or communicate the information, that party may use or disclose it only to the extent permitted by law. Within a reasonable time after the commercial transaction is completed, the organization that obtained the personal information must notify the individual that it now holds their personal information as a result of the transaction.

Employment relationships. It should be noted that Bill 64 does not introduce a consent exception for the collection, use or communication of personal information to establish, manage or terminate an employment relationship. Indeed, an amendment to introduce an exception similar to that provided for in PIPEDA and the British Columbia and Alberta PIPAs was unfortunately rejected. The absence of such an exception may create challenges for employers given the limitations of the consent model in the context of employer/employee relationships. It is generally difficult to consider an employee's consent to be "freely" given in this context, since an employee may believe, correctly or incorrectly, that their employment would be jeopardized by a refusal to consent. Moreover, if employees refuse to allow their employer to collect, use or communicate personal information for routine business practices, this may prevent the employer from carrying on its business and fulfilling its legal obligations.

Steps to compliance

1. **Prepare an inventory of uses that may be exempted from the consent requirement** to determine whether they fall within the following exceptions:
   - Use necessary for the supply or delivery of a product or the provision of a service requested by the individual.
   - Use necessary for the prevention and detection of fraud.
   - Use necessary for the evaluation and improvement of protection and security measures.
   - Use clearly for the benefit of the individual.
   - Use consistent with the purposes for which the information was collected.
   - Use necessary for study or research purposes or for the production of statistics to the extent that the information is de-identified.

2. **Prepare an inventory of communications that may be exempted from the consent requirement** to determine if they fall within the following exceptions:
   - Communication necessary for carrying out a mandate or performing a contract of enterprise or for services.
   - Communication to a person or to an organism that wishes to use the information for study or research purposes or for the production of statistics.

→ Continued on next page

Steps to compliance

3. **Review privacy notices and consent forms to:**
    - Reflect the exceptions to the consent requirement and structure these documents so that uses or communications exempt from consent are better reflected.

4. **Implement a procedure to manage communications of personal information in a commercial transaction context** to ensure that:
    - The commercial transaction falls within the exception to the consent requirement in the Private Sector Act.
    - Any communication of information is necessary for the conclusion of the commercial transaction in question.
    - An agreement is reached with the other party, stipulating that the latter undertakes: (i) to use the information only for the purpose of completing the commercial transaction; (ii) not to communicate the information without the individual's consent; (iii) to take the necessary measures to ensure the protection of the confidentiality of the information; and (iv) to destroy the information if the commercial transaction is not completed or if its use is no longer necessary.
    - When the commercial transaction is concluded, ensure that within a reasonable period of time after the conclusion of the commercial transaction, the individual concerned is notified of the transaction by the organization that now holds their information.

4. Research, internal analytics and automated decision-making

Bill 64 introduces welcome reforms to the regime governing the use of personal information in the context of research for public good, better aligning Québec with the frameworks established in other Canadian jurisdictions.

The amendments also introduce important new flexibilities to the regime governing the use of personal information in the context of secondary internal research purposes, such as enterprise analytics, by clearly permitting the use of "de-identified" personal information (including sensitive information) within the enterprise without obtaining consent.

The amendments also set out important new obligations in relation to the use of technologies involved in automated decision-making, which, while undefined, is clearly directed at machine learning and other "artificial intelligence" technologies capable of making sophisticated decisions without human supervision.

4.1. Consent exception for research

Effective September 22, 2022

Bill 64 eliminates the authorization process for research, long criticized for its impracticality and for the uncertainty created by the CAI's discretion over the assessment of requests for research authorizations and its power to revoke authorization.

The amendments to section 21 and the introduction of new sections 21.0.1 and 21.0.2 of the Private Sector Act replace the current process with a regime that allows parties to a transfer of personal information for research purposes to make the assessment themselves. The new framework emphasizes due diligence and transparency, and only requires that the CAI be notified of the agreement entered into between the disclosing and recipient organizations, and of breaches of the agreement or events that could breach the confidentiality of the personal information.

Privacy impact assessment. The new section 21 states that the information may be communicated if a PIA concludes that: (i) the personal information is needed to achieve the objective; (ii) it is unreasonable to require the requesting person or body to obtain consent from the individual concerned; (iii) the objective of the research outweighs the impact on individual privacy in light of the public interest; (iv) the information is used in a manner that ensures its confidentiality; and (v) only necessary information is communicated (s. 21 para. 2). The organization transmitting the personal information is responsible for completing the PIA, based notably on the information obtained by the requesting party.

Disclosing organizations should therefore be prepared to estimate their costs for undertaking an assessment, which will typically need input from the disclosing organization's legal department or external counsel. The cost of conducting a PIA (whether alone or in cooperation with another

entity) can be significant. However the agreement with the requesting person or body is structured, the disclosing organization's costs should be accounted for in the arrangement. The disclosing organization however, has the discretion to withhold the requested personal information, even without completing a PIA.

Requesting organizations will therefore also likely need to budget for the cost of compensating the disclosing organization. This may have the unintended consequence that it will be difficult for smaller, less-well-funded projects to obtain the information needed without agreeing to alternative forms of compensation, such as priority access to analyses or favourable licensing terms for intellectual property arising from the research.

Obligations for requesting persons. For its part, the person or body wishing to use the personal information must make the request in writing and provide the disclosing organization with comprehensive information relating to the request. This will include a detailed presentation of the research activities, the grounds supporting fulfilment of the criteria for the PIA referred to in section 21, a list of all other persons and bodies of which a similar request is being made, and if applicable, the technologies to be used in processing, and the documented decision of a research ethics committee relating to the research (if applicable) (s. 21.0.1).

In order to avoid the potential for a negative finding relating to due diligence prior to making the disclosure, the disclosing organization should ensure that the requesting person or body has furnished all of the applicable information and support set out at section 21.01. If the recipient organization, researcher or public body experiences a data breach involving the information disclosed (see section 7.2), the disclosing organization may come under scrutiny by the regulator in the course of the investigation.

Mandatory agreement provisions. The two parties to the transfer of information must also enter into an agreement 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 research activities;
- may not be matched with any other information file that has not been provided for in the detailed presentation of research activities; and
- may not be communicated, published or otherwise distributed in a form allowing the persons concerned to be identified.

The agreement must also:

- specify the information that must be provided to the persons concerned if personal information concerning them is used to contact them to participate in the study or research;
- provide for measures for ensuring the protection of the personal information;

- determine a preservation period for the personal information;
- set out the obligation to notify the person who communicates the personal information of its destruction; and
- provide that the person who communicates the personal information and the CAI must be informed without delay (i) of non-compliance with any condition set out in the agreement; (ii) of any failure to comply with the protection measures provided for in the agreement; and (iii) of any event that could breach the confidentiality of the information (s. 21.0.2).

Submission of agreement to the CAI. The agreement must be sent to the CAI and only comes into force 30 days after it is received by the CAI (s. 21.0.2 para. 3). While the provisions of section 21.0.2 do not grant the CAI the power to resiliate the agreement if it fails to fulfil all of the requirements, the CAI could nonetheless order the transfer not to proceed until the agreement is revised to include the stipulated elements, and it could also suspend the agreement or exercise its other supervisory powers under the Act. The CAI may contact the parties during or after the 30-day period.

Steps to compliance

1. Implement a procedure for research projects under which :

- The disclosing party will ensure that it has received all applicable required information specified at section 21.01 prior to making any disclosure.
- A PIA will be prepared prior to making any disclosure, and an assessment will be made of the cost of doing so and consider how those costs and other due diligence costs should be handled between the parties.
- An agreement that fulfils the requirements of section 21.0.2 will be executed.

2. Deliver a copy of the agreement to the CAI at least 30 days prior to exchanging the information.

4.2. Consent exception for internal research and analytics

Effective September 22, 2023

Bill 64 amends section 12 of the Private Sector Act to state that personal information initially collected for one purpose may be used within an organization, without consent, for (i) purposes consistent with the purposes for which it was collected (s. 12 para. 2(1)) and (ii) study or research or for the production of statistics, if the information is de-identified (s. 12 para. 2(3)).

Consistent purposes. Section 12 paragraph 2(1) permits organizations to use personal information for an additional or secondary purpose without consent provided that it is for a consistent purpose, defined as a purpose having a "direct and relevant connection with the purposes for which the information was collected", and provided that the purpose is not "commercial or philanthropic prospection" (i.e. marketing). The language used echoes the phrasing used in certain public sector privacy laws of other Canadian jurisdictions and faintly echoes the GDPR's "compatible purposes" language.

While the introduction of this consent exception opens the door for organizations to use personal information in its native form for research and analytics, organizations should exercise caution. The CAI may consider whether the consistent use falls within the reasonable expectations of the individual in relation to the original purpose, rather than whether it is objectively reasonably compatible but might not have occurred to the individual. The more sensitive the information at issue, the more likely it is that the regulator will lean towards a "reasonable expectations" perspective in its analysis.

For example, using non-sensitive personal information in analytics that will improve or optimize services not only for the individual concerned but also other users of the same service might fall within the scope of consistent purposes, provided that the organization stated in its privacy notices that it would use personal information to optimize or improve services. Using highly sensitive information for the same "general improvement" analytics may fall outside what the CAI considers as reasonably expected by individuals. In such cases, using de-identified personal information as input for the research and analysis (as also provided for under section 12 and discussed below) would be a more prudent choice.

Study or research if information is de-identified. Section 12 paragraph 2(3) provides for the use of personal information without consent where its use is "necessary for study or research purposes or for the production of statistics and if the information is de-identified." Given that the consent exception applies to use within the enterprise, it is natural to construe "study or research" as including enterprise or business analytics. However, it also encompasses other forms of internal research activity which could include machine learning or other advanced information analysis techniques that could lead to the development of automated decision systems (discussed further in 4.3).

We note that while this is an exception to consent, it is not expressly an exception to knowledge and consent. That said, the other exceptions to consent listed in section 12 occupy a spectrum on which the lack of knowledge runs from being relatively benign for the affected individual (e.g. if the information is used for the benefit of the individual) to being beneficial for all individuals and the organization (e.g. the prevention and detection of fraud). In consequence, it cannot be assumed that the consent exceptions listed in section 12 carry a general implication that individuals will be given notice of the use. This is particularly important given that the use of such information in unsupervised machine learning contexts can lead to the discovery of new purposes which could not reasonably be articulated in advance.

The amended section states that personal information is "de-identified if it no longer allows the person concerned to be directly identified" (s. 12 para. 4(1)). This aligns with the core features of the notion of pseudonymized information, as this term is generally understood (including under the GDPR). Underscoring this understanding of de-identification, Bill 64 also introduces criteria for anonymization, stating "[f]or the purposes of this Act, information concerning a natural person is anonymized when it is at all times reasonable to expect in the circumstances that it irreversibly no longer allows the person to be identified **directly** or **indirectly**" (s. 23, emphasis added). Interestingly, the language of the new section 12 also clearly provides that no consent is needed even where such information is sensitive (s. 12 para. 1 and 2).

The amended section 12 also recognizes that there is a risk of re-identification attached to de-identified information, stating that organizations that use de-identified information "must take reasonable steps to reduce the risk of anyone identifying a natural person using de-identified information." (art. 12 para. 5). Although not expressly stated, it would be consistent with the definition of sensitive information provided in section 12 (as well as the guidance of the CAI and other Canadian privacy regulators) to interpret the "reasonable steps" as including additional or more aggressive measures when the personal information underlying the de-identified information is sensitive.

Privacy impact assessments. Such internal research, whether conducted under s. 12, paragraph 2(1) or 2(3), may call for a privacy impact assessment if it is directed at a "project of acquisition, development and redesign of an information system project or electronic service delivery" (see section 2.3).

Steps to compliance

1. **Develop and implement a procedure to ensure that the organization has, when using personal information for internal research, either:**
   - obtained consent for that use;
   - ensured that the research purpose is consistent with a purpose for which the information was collected; or
   - de-identified (i.e. at minimum pseudonymized) the personal information.
2. **Exercise caution when using the "consistent purposes" exception to support the use of sensitive personal information in internal research.** When information is sensitive, the CAI may be more inclined to consider whether the consistent use falls within the reasonable expectations of the individual in relation to the original purpose, rather than whether it is objectively reasonably compatible but might not have occurred to the individual.
3. **Take reasonable steps to reduce the risk of re-identification** when using de-identified information under the "study and research" exception.
4. **Implement more stringent measures to avoid re-identification** where the personal information underlying the de-identified information is sensitive.
5. **Develop and implement a procedure to undertake the preparation of a privacy impact assessment** if the internal research (under either of the exceptions discussed) is directed at a "project of acquisition, development and redesign of an information system project or electronic service delivery" (s. 3.3.).

4.3. Automated decision-making

Effective September 22, 2023

The new section 12.1 introduces notice obligations for organizations that use personal information to make a decision about an individual when such decisions are based **exclusively** on automated processing of such information. This could include, for example, situations where an organization decides whether to grant or refuse access to a product or service based on an assessment of an individual's financial or medical situation.

Notice and information requirements. Section 12.1 requires organizations to inform individuals when their personal information is used to render a decision based exclusively on automated processing of such information, no later than at the time the individual is informed of the decision itself. This creates some flexibility as to the exact timing of the notice. For instance, an organization may choose to provide this notice at the time of collection, rather than at the time the decision is made, assuming, of course, that there is an actual delay between the two. As a practical matter, in addition to more detailed notices and / or "just in time" notices that might be required pursuant to future CAI guidance, organizations using technologies to make decisions based exclusively on automated processing should indicate the use of such technologies in general terms in their privacy notices.

Section 12.1 also requires that upon request, organizations must inform individuals about whom such a decision has been made:

- of the personal information used to render the decision;
- of the reasons and the principal factors and parameters that led to the decision; and
- the right to have the personal information used to render the decision corrected.

It is interesting to note that the phrasing used does not limit these rights to the personal information that is about the affected individual. It is not clear whether this is intentional, given the context: machine learning technologies that make decisions about individuals may need to ingest large quantities of personal information of many individuals in order to yield a model capable of making accurate decisions. While no interpretation of the law would require personal information of other individuals to be disclosed to an individual affected by the decision of such a system, it is conceivable that organizations will be expected to disclose the nature of all personal information used (e.g. the fact that the training phase used the names of convicted criminals and the postal codes of their place of residence). The phrasing "inform such individual of the personal information used…" is ambiguous in this respect. Guidance from the CAI will be of critical importance here in understanding how these obligations to inform should be parsed.

"Automated processing" is not defined under Bill 64. Guidance from the CAI is therefore of critical importance here as well. While the target of Bill 64's amendments may well be automated decision-making that has a significant effect on individual rights, with a focus on artificial intelligence ("AI") technologies, the drafting is broad enough that all sorts of other automated processes that make "decisions" could be caught up in its scope. For example, the provisions do not exclude the decision of an automated process to expose an individual to an offer for a product or service based on their online activity or perceived interests as reflected by previously assembled profiling information (i.e. targeted advertising).

The CAI has listed automated processing as one of the themes in its "espace évolutif" for Bill 64, signalling that the CAI intends to issue guidance on this point. It is therefore reasonable for organizations to expect such guidance before section 12.1 enters into force. It bears mentioning that the term "automated processing" appears to be imported from the European Union's ("EU") GDPR and is likely intended to be interpreted in a similar fashion. In Europe, the Article 29 Data Protection Working Party (responsible for many of the core interpretations of the GDPR), set out extensive guidance on the interpretation of the GDPR's provisions governing automated processing prior to the law's entry into force (see Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679). We note that in the Working Party's case, its interpretative efforts benefited from the GDPR's limiting language concerning automated processing, which focuses attention on processing that "produces legal effects concerning him or her or similarly significantly affects him or her". The amendments introduced by Bill 64 have no such limiting language, which will no doubt complicate the interpretative work of the CAI. In the absence of guidance, however, in order to prepare for the law's new notification and information disclosure obligations, organizations may cautiously consider guidance from the European context for determining whether and in what circumstances a technology will qualify as automated processing.

The legal obligation to provide "the reasons" that led to the decision is tantamount to requiring that the decision be explained. As commented on extensively in the literature on AI, the processes by which machine learning models reach their conclusions are notorious for resisting explanation. The kind of explanation that can be offered, in many cases, will be either superficial to the point of vacuity or so particular as to have no explanatory value for the average individual (or experts, for that matter). The mention of "principal factors and parameters" offers a small clue as to the level of detail required, but in the absence of further guidance, organizations must be cautious in disclosing details that may (i) disclose trade secrets or intellectual property of the organization or of third parties (such as service providers that provide the automated processing technology) or (ii) enable fraudsters to game the system.

Individual right to submit observations. In addition, concerned individuals must be given the opportunity "to submit observations to a member of the personnel of the organization who is in a position to review the decision made by automated means". Automated processing activities that affect individuals must hence, upon request, be reviewed by personnel who have the power (and, presumably, sufficient knowledge) to re-assess computer-made decisions. Interestingly, section 12.1 does not grant individuals a right not to be subject to decisions based solely on automated processing (such as the one granted in the GDPR, at article 22) but rather only the right to "an opportunity to present observations". This appears to grant the reviewer latitude to approve the automated decision following receipt of the observations – that is, the reviewer has no separate obligation to deliberate and come to an independent conclusion, or provide any reasons as to why a new decision should be reached or the original decision should stand. As such, it is not clear how or to what extent the reviewer must consider an individual's observations when reviewing the decision. Organizations will therefore be able to triage meritless complaints without extensive administrative overhead. Nonetheless, organizations must be prepared to assess observations submitted, and act appropriately when review of the decision and observations clearly signals a problem in the processing mechanism or the way in which the personal information is used.

Steps to compliance

1. **Prepare to act upon guidance to be issued by the CAI on how "automated processing" should be interpreted.** In the absence of such guidance, organizations may cautiously consider the interpretation of "automated processing" as provided for under the EU's GDPR.
2. **Implement a procedure to ensure that if an organization renders decisions based exclusively on an automated processing:**
   - individuals will be notified via the organization's privacy notices in general terms.
   - the procedure as set out in the "Steps to Compliance" for Section 5 will be in effect.
3. **Exercise caution when disclosing reasons for the decision that may:**
   - reveal trade secrets or intellectual property of the organization or of third parties (such as service providers that provide the automated processing technology).
   - enable fraudsters to game the system.
4. **Prepare to assess observations submitted** and act appropriately when review of the decision and observations clearly signals a problem in the processing mechanism or the way in which the personal information is used.

5. New individual rights

Individuals are granted three new rights under Bill 64: a right to control the dissemination of their personal information (also known as "the right to be forgotten"); a right to data portability; a right to be informed of, and submit observations on automated decision-making. In addition, Bill 64 reinforces individual control and existing privacy rights by enabling individuals to request further information from organizations about their data processing.

5.1. Right to be forgotten

Effective September 22, 2023

Bill 64 affords individuals the right to control the dissemination of their personal information by organizations and online intermediaries who facilitate the dissemination of such information. This right is more commonly known as the right to be forgotten, and its primary purpose is to enhance an individual's control over their online reputation and privacy by restricting the public's access to personal information where its dissemination is either unlawful (e.g. revenge porn) or causes serious harm to the reputation or privacy of an individual. Unlike an equivalent right found in the EU's GDPR, Québec's new right to be forgotten is not a right of erasure of personal information per se, but rather a more limited right to restrict the dissemination of information. We should note in passing that the right to request deletion of personal information is maintained under Bill 64 in accordance with section 28 of the Private Sector Act and article 40 of the Civil Code. For more details on the right to request deletion, please refer to our bulletin *The right to erasure of personal information in Canada: Between fact and fiction*.

Scope of the right to be forgotten. Under this new right, an applicant can restrict organizations from disseminating their personal information or can have hyperlinks associated with their name and that provide access to personal information, de-indexed (or, to put it more accurately, "delisted" from search results) where the dissemination of the personal information (i) contravenes the law or a court order, or (ii) otherwise causes serious injury to the individual's reputation or privacy (s. 28.1). In practice, this means that an organization that receives this type of request must not only conclude that the injury actually exists and is not merely hypothetical or potential, but also that it outweighs the public's right to information and the freedom of expression of the publisher or creator of content, and that the remedy being requested is not excessive in terms of preventing the perpetuation of the injury. To make this assessment, the organization must specifically consider a number of prescribed factors, which closely mirror those elaborated in decisions involving defamation or privacy-related claims. These factors include:

- The public status of the individual;
- The fact that the information concerns an individual while they were a minor;
- The accuracy, currency and sensitivity of the personal information being disseminated;
- The context of its dissemination;

- The time elapsed since it was published; and
- If the information relates to criminal matters, the existence of a pardon or restriction on the access of criminal records.

Interestingly, this new right also grants the ability to "re-index" hyperlinks associated with an individual's name where doing so can prevent the perpetuation of a serious injury to an individual's reputation or privacy. According to statements issued by Minister Sonia LeBel – who originally introduced Bill 64 – the right to have hyperlinks re-indexed was described as a right to "move" a hyperlink, which potentially raises a number of practical challenges.

Format of the request. An organization has an obligation to consider only requests that have been made in writing by a person who proves that they are the individual to whom the personal information relates or an authorized representative, such as a person holding parental authority (s. 30). Although the Private Sector Act affords heirs, successors, liquidators of a succession and a number of other individuals the ability to exercise the privacy rights of a deceased person, it is not readily clear whether this extends to the right to be forgotten itself.

Evaluating the merits of the request. Considering that the applicant is generally in a better position to bring forward evidence in support of their request, the latter may bear the initial burden of establishing that the dissemination of the personal information is in fact unlawful or otherwise causes serious injury to their reputation or privacy. However, further regulatory guidance may be required to confirm this point. The organization receiving this request must then exercise due diligence in assessing the request's overall validity and seek clarification from the applicant where appropriate. Whether this extends to conducting an independent investigation or fact-gathering exercise remains to be seen, but is likely to raise broader questions about the role of private-sector entities in deciding what information the public has a legitimate interest in accessing. As this role has been traditionally fulfilled by courts, which are generally in a better position to resolve complex questions of fact and of law and are subject to various procedural safeguards meant to protect competing fundamental rights, challenges to the constitutionality of Bill 64's new right to be forgotten could eventually arise.

Delay to respond to the request. The Privacy Officer must respond to the request in writing within 30 days of its receipt (s. 32). However, the organization may submit a request to the CAI within this initial 30-day period to extend the time limit within which it must provide its response (s. 46). Unlike other Canadian data protection laws, no upper limit is placed on the total number of days by which the CAI can extend the time limit.

Granting the request. Where the request is granted, the Privacy Officer must respond in writing and provide an attestation that the information is no longer being disseminated or that the hyperlink has been de-indexed or re-indexed, as applicable (s. 28.1 para. 5).

Refusing the request. Where the request is refused, the Privacy Officer must respond in writing, provide reasons for the refusal, indicate the provision on which the refusal is based (if any), and inform the applicant of their remedies and the time limit for exercising them (s. 34). On this last point, the organization must inform the applicant of their right to submit an application for the examination of a disagreement to the CAI within 30 days of the refusal to grant the request (s. 43). If so requested by the applicant, the Privacy Officer must also help them understand the refusal.

Outstanding questions. While Bill 64's right to be forgotten is ostensibly directed towards online search engines and content publishers, the situation may be less clear with respect to online intermediaries (such as a social media platform) who merely facilitate the dissemination of user-generated content without otherwise taking an active role in its publication. Whether they can be said to "disseminate" the information that flows through their platforms raises important questions about their role and responsibilities in monitoring user-generated content, particularly in light of the protections afforded under sections 22 and 27 of Québec's *Act to establish a legal framework for information technology* ("**IT Act**"). On this last point, the Québec Superior Court in *Lehouillier-Dumas* c. *Facebook inc.*, 2021 QCCS 2074, has offered valuable insights into these broader issues.

5.2. Right to data portability

Effective September 22, 2024

Treated as an extension of the right of access, data portability grants individuals a supplementary right to receive computerized personal information collected from them in a **structured, commonly used and technological format** and to have this information transferred directly to "any person or body authorized by law to collect such information" (s. 27 para. 3). This information must also be communicated in the form of a **written and intelligible transcript** (s. 27 para. 2). Thus, the objective of the data portability right is to facilitate the reuse of data and to enhance the ability of consumers to switch providers, thereby enhancing individual control over their personal information and promoting greater competition. While the data portability right does not necessarily seek to achieve interoperability between systems, this is often framed as one of its underlying aims.

Meaning of "structured, commonly used and technological format". The terms "structured", "commonly used" and "technological" are not explicitly defined within the law, and their meaning is likely to vary depending on the industry or sector involved. In the EU, the former Article 29 Working Party issued guidance in which it held that open formats such as CSV, XML and JSON, accompanied by metadata useful to understanding its meaning, were compliant with the GDPR's data portability right where no commonly used format was available. That said, further regulatory guidance will be needed to confirm which formats may be viewed as compliant under Bill 64.

Scope of the data portability right. The data portability right applies only to computerized personal information that was collected from the individual. In other words, it does not apply to information held in a non-computerized format, such as paper documents, or collected from a third party. To protect the commercial interests of businesses, including proprietary models used to generate information, the data portability right expressly excludes from its scope personal information that was created or derived from information collected from an individual. For instance, this may include inferences about a customer's likelihood to purchase certain products or services or their likelihood to be interested in receiving particular media content. It should be noted that the implementation of this right must also be taken into account prior to the acquisition, development or overhaul of an information system or electronic service delivery system involving the processing of personal information (s. 3.3 para. 3) (see section 2.3). While greater clarity is needed with respect to some of the procedural aspects associated with the data portability right, its inclusion under the right of access suggests that organizations should handle data portability requests in accordance with the current regime applicable to access requests.

Exemptions to data portability. Where the provision of the information in a structured, commonly used and technological format "raises serious practical difficulties" for the organization receiving the request, the latter may be exempted from having to comply with this requirement. Moreover, the data portability right may not apply to information that is otherwise exempt from the right of access, as data portability is treated as an extension of the latter (see ss. 37 to 41). In this sense, computerized personal information whose disclosure would be likely to reveal personal information about a third person is likely to be exempt from both access and portability requirements pursuant to section 40 of the Private Sector Act.

Finally, it is important to note that the right to data portability will come into effect only on September 22, 2024, that is three years after Bill 64's enactment.

5.3. Right to be informed of, and submit observations regarding automated decision-making

Effective September 22, 2023

Bill 64 grants individuals three new rights in relation to automated decision-making involving personal information, namely (i) the right to be informed thereof, (ii) the right to request additional information on automated decision-making, and (iii) the right to submit observations to a designated person within the organization. It bears emphasizing that these rights are limited to decisions based "exclusively" on an automated processing of an individual's personal information, thereby excluding decisions based on a combination of automated processing and meaningful human involvement.

Right to be informed of automated decision-making. Individuals are afforded a right to be informed of the fact that their personal information is used to render a decision based exclusively on automated processing. See section 4.3 for more details on this new requirement.

Right to request additional information on automated decision-making. Individuals may also request additional information on automated decision-making. In particular, they may request information about the personal information that was used to render the decision, the reasons and principal factors and parameters that led to the decision, and their right to have personal information rectified. See section 4.3 for more details on this new requirement. Given that there are no modalities imposed on the exercise of the right to request additional information, an individual may be entitled to submit a request verbally or in writing. The organization should nevertheless act with diligence and maintain a record of this type of request, including the organization's response thereto, as a failure to comply with this requirement – or any of the other rights afforded under section 12.1 – could give rise to the imposition of administrative monetary penalties (s. 90.1(4)) (see section 1).

Right to submit observations to a designated person within the organization. Individuals must be afforded an opportunity to submit observations to a member of the personnel of the organization, and this designated person must be in a position to review the decision. See section 4.3 for more details on this new requirement.

5.4. Right to request information about data processing

Effective September 22, 2023

Bill 64 grants individuals the ability to request information about data processing, namely what personal information was collected from them and how it is being processed by the organization. In particular, an individual could request not only the information that was provided to them at the time of collection but also additional information, such as the categories of persons who have access to their personal information within the enterprise, the applicable retention period, and the contact information of the Privacy Officer (s. 8). If an individual's personal information was collected from a third person, the individual may similarly request to be informed of the source of the information unless the information was collected for an inquiry to prevent, detect or repress a crime or statutory offence (s. 7). For more details on these requirements, please refer to section 3.1. Other Canadian data protection laws provide individuals with a similar right to request information about data processing. However, this right falls within the scope of the access right, meaning that an organization who receives this type of request must handle it in accordance with the procedure and delays applicable to an access request. In contrast, Bill 64 separates these two rights, thereby creating a more flexible regime for requests made pursuant to sections 7 and 8. It is nevertheless recommended to act with diligence, as a failure to inform individuals in accordance with these provisions is one of the enumerated situations that expressly give rise to the imposition of administrative monetary penalties (s. 90.1(1)) (see section 1).

Steps to compliance

1. **Prepare an inventory of practices that may trigger the application of new individual rights** to identify whether such practices fall within any of the following situations:
   - The organization disseminates content that may include personal information or operates an online search tool or similar indexation service that generates search results (in the form of hyperlinks) based on an individual's name.
   - The organization renders decisions based exclusively on an automated processing of personal information.
   - The organization collects computerized personal information from individuals.
2. **Prepare an inventory of existing policies and procedures for handling privacy requests** or any similar document (clients or employees) **and review them** to ensure that:
   - The organization is able to recognize and respond to a request (verbal or written) for information about data processing.
   - The organization is able to furnish computerized personal information to the individual, or a person or body authorized by law to collect such information, in a structured, commonly used and technological format upon request.

→ Continued on next page

Steps to compliance

3. **If it renders decisions based exclusively on automated processing, implement a procedure to ensure that:**

   - The organization is able to inform individuals (clients or employees) of this fact no later than at the time it informs them of the decision.
   - The organization is able to recognize and respond to a request (verbal or written) for information about automated decision-making.
   - The organization has designated a member of its personnel who is in a position to review these decisions to be responsible for receiving observations from individuals.

4. **If it disseminates personal information or operates an online search tool, implement a procedure to ensure that:**

   - The organization is able to receive, evaluate and respond to a right to be forgotten request in accordance with prescribed delays.
   - The organization has a process in place to determine whether the dissemination of personal information (i) contravenes the law or a court order or causes serious injury to an individual's reputation or privacy; and (ii) if applicable, causes injury that outweighs the public's right to information and the freedom of expression of the publisher or content creator.
   - The organization is able to verify the identity of the applicant making the request (in compliance with applicable laws).
   - The organization is able to provide attestations (if the request is granted) that the information is no longer being disseminated or that the hyperlink has been de-indexed or re-indexed, as applicable.

6. Outsourcing and transfers outside of Québec

Bill 64 introduces new requirements for outsourcing and communicating of personal information outside Québec.

6.1. Outsourcing

Effective September 22, 2023

Openness. As noted in section 3.1, Bill 64 requires the organization to inform the individual, at the time of collection and subsequently upon request, of the names of the third parties or categories of third parties to whom the information is to be disclosed for the purposes described in the organizations's privacy policy (s. 8 para. 2). This means that the organization's privacy notice will have to indicate that personal information may be transferred to its service providers (category of third parties) or name them individually.

Exception to consent. As noted in section 3.3, Bill 64 permits the disclosure of personal information to a third party without the consent of the individual, where such disclosure is necessary for the performance of a mandate or the execution of a contract for services (s. 18.3). This exception therefore allows the organization to transmit personal information to its agents and service providers ("**service providers**") without the individual's consent.

Requirement to conduct a PIA. Where an outsourcing project involves the acquisition, development and redesign of an information system or electronic service delivery involving the collection, use, communication, keeping or destruction of personal information by a service provider on behalf of the organization, the organization will be required to conduct a PIA (s. 3.3(1)). While this is the responsibility of the organization, the service provider should cooperate in this exercise. We refer to section 2.3 for PIA requirements.

Written agreement. Bill 64 further requires that the processing of personal information by an agent or service provider be subject to a written agreement that must include the steps the service provider must take to ensure:

- the protection of the confidentiality of the personal information disclosed. The agreement should provide for the physical, organizational and technical measures to be put in place by the service provider handling the information, whether it is in transit or in storage;
- that the information will only be used for the purpose of performing the service contract. The agreement should prohibit the use of personal information by the service provider for its own purposes or for the purposes of a third party. It would be useful to clarify whether the new exceptions to consent in section 12 would nonetheless permit the service provider to use the information for the purposes described therein (e.g. de-identifying the information for its internal purposes, research or statistical production).

- that the service provider will not retain the personal information after the contract expires. Bill 64 does not specify whether the de-identification of such information by service providers for use in furtherance of their serious and legitimate purposes (s. 23) would satisfy this requirement.

Requirement to notify breaches of confidentiality obligations. Section 18.3 requires the service provider to promptly notify the organization's Privacy Officer of "any breach or attempted breach by any person of any of the obligations concerning the confidentiality of the information communicated", not simply confidentiality incidents. It is unclear whether the parties will be able to adjust the terms of the obligation, if any, to limit the notification obligation to "confidentiality incidents".

Authorize audits by the organization. The service provider must allow the organization's Privacy Officer to conduct any audit related to the service provider's confidentiality obligations, i.e. to request any documents and to conduct any additional audits. It is unclear whether the parties will be able to tailor the conditions to which these obligations will be subject, for example by requiring that audits be conducted at certain times or be subject to certain conditions.

These two obligations (written agreement and obligation to notify violations of confidentiality obligations) do not apply when the service provider is a public body within the meaning of the *Act respecting Access to documents held by public bodies and the Protection of personal information* or a member of a professional order
(s. 18.3 para. 3).

Steps to compliance

1. **Privacy Policy.** Review the organization's privacy policy to ensure that it indicates that personal information may be shared with its service providers. If the organization wishes, the policy can name these service providers.
2. **Develop an outsourcing procedure** that governs employees that may be outsourcing the processing of personal information (such as employees part of the procurement team).
3. **Prepare a contract (or clauses) template for the processing of personal information.** This contract should provide for the following:
   - The protection of personal information;
   - The use of personal information for the purpose of fulfilling the contract;
   - The destruction of the information at the termination of the contract;
   - A requirement by the service provider to promptly notify the organization of any breach or attempted breach of confidentiality obligations; and
   - The right for the organization to request any document and to carry out any verification relating to the confidentiality of the personal information.

→ Continued on next page

Steps to compliance

4. **Identify service providers that process personal information for the organization.** The organization will then need to:
    - Determine whether a written contract that meets the requirements of step 2 has been entered into with each service provider; and
    - If not, require that the contract template described in step 2 is entered into by the relevant service providers.

5. **Contact existing service providers whose systems/services require the organization to conduct a PIA.** Based on the list in step 3 above, the organization should plan to:
    - Communicate with each existing service provider that the organization wishes to get involved in the acquisition, development or redesign of information systems or electronic service delivery involving the collection, use, communication, keeping or destruction of personal information to inform them that the organization will be conducting a PIA for which it will require their cooperation; and
    - Once the PIA template has been developed by the organization, it should be shared with the service provider to assist the organization in completing the factual and technical information for the systems/services involved.

6. **Conduct PIAs.** A PIA shall be conducted by the organization for each outsourcing project involving the acquisition, development or redesign of an information system or electronic service delivery involving the collection, use, communication, keeping or destruction of personal information.

6.2. Transfers outside of Québec

Effective September 22, 2023

Transparency. As indicated in section 3.1, an organization that collects personal information from individuals must inform them of the possibility that this information may be disclosed outside Québec (and not just Canada). This information must be provided at the time of collection and upon request (s. 8 para. 2).

Privacy Impact Assessment ("PIA"). Transfers of personal information outside Québec are a major concern of Bill 64, which introduces restrictions on transfers in section 17. Thus, an organization that (1) wishes to transfer personal information outside Québec or (2) entrusts a third party located outside Québec with the task of collecting, using, disclosing or retaining personal information on its behalf is required to conduct a PIA that takes into account the following factors:

- The sensitivity of the information
- The purposes for which it will be used
- The safeguards, including contractual safeguards, that will be applied, and
- The legal regime applicable in the receiving state, including the privacy principles applicable there. It should be noted that Bill 64 refers to "principles", not to a data protection "law".

If the PIA "demonstrates that the personal information would be adequately protected, including with respect to generally accepted privacy principles" then the transfer will be authorized. Note that the Act does not specify what "generally accepted data protection principles" are. One may wonder if this notion refers to the personal protection principles listed in the *Guide to Conducting a PIA* (in French only) issued by the CAI on March 10, 2021, namely:

- Determine the purpose of the collection;
- Limit the collection of personal information;
- Inform the person concerned;
- Implement appropriate security measures;
- Limit access to personal information;
- Limit the use of personal information;
- Obtain consent to communicate personal information;
- Obtain consent from the persons concerned;
- Ensure the quality of personal information;
- Allow access and rectification rights;
- Respond with diligence.

This new approach is similar to the requirements of the GDPR, which require the organization transferring personal data to a jurisdiction outside the European Economic Area that has not been recognized as adequate by the European Commission to conduct a transfer risk assessment before transferring the data abroad (see on this point the Recommendations 01/2020 and 02/2020 of the European Data Protection Board) and adds if necessary any additional protective measures to the standard contractual clauses adopted by the European Commission.

Written contract. If the PIA demonstrates that the information processed abroad will be adequately protected, the organization must enter into a written agreement with the third party that takes into account, among other things:

- The results of the PIA and,
- The terms and conditions, if any, agreed to in order to mitigate the risks identified in the assessment (s. 17 para. 2).

Thus, if the PIA concludes that information processed abroad by a service provider will be sufficiently protected with a contract that incorporates the requirements of section 18.3, no further action will be necessary. If, on the other hand, the assessment concludes that the processing abroad creates a risk to its protection, then the parties will have to agree on measures to reduce that risk to an adequate level. Bill 64 does not specify what such measures would consist of, but it is conceivable that technical (e.g. encryption, de-identification), organizational and contractual measures (e.g., restrictions on sharing information with foreign government authorities) might be able to mitigate the level of risk. The Act also does not specify what would happen if the outcome of the PIA was unfavorable, suggesting that the transfer could not proceed.

Steps to compliance

1. **Review the organization's privacy policy to clarify that personal information may be disclosed outside of Québec (not just Canada).**
2. **Map transfers outside of Québec.** This exercise will provide a description of information flows. Among other things, the organization will need to verify:
   - The address of the service provider involved in the communication;
   - The terms and conditions under which the affiliates and/or subcontractors of the provider located in other jurisdictions will be able to access the information (e.g. in the context of a service outsourced to an affiliate located in a third country); and
   - The nature and volume of personal information processed outside Québec.
3. **Complete the PIA template to evaluate the risks associated to the communication of personal information outside Québec.** This template will need to take into account:
   - The sensitivity of the information communicated;
   - The purposes for which it will be used;
   - The safeguards, including contractual ones, that will apply to it; and
   - The legal regime applicable in the receiving state.

→ Continued on next page

Steps to compliance

4. **Conduct a PIA for processing activities involving the communication of personal information outside Québec.** This exercise will notably have to assess whether the legal framework of each jurisdiction where the personal information is processed includes privacy principles that are consistent with "generally accepted privacy principles."
    - As a first step, in the absence of more specific guidance on this point, organizations may wish to consider whether the legislation of the state in question respects the privacy principles listed in the *Guide to Conducting a PIA*.
5. **Adapt the contract (or clauses) template for processing personal information to take into account the requirements of service providers located outside Québec.** This template must:
    - Reflect the requirements of section 18.3 described in section 6.1 – step 3, and
    - Provide safeguards that can be adapted based on the results of the PIA.
6. **Prepare a contract (or clauses) template with third parties non-service providers located outside of Québec.** The template must:
    - Require third parties to comply with generally accepted privacy principles; and
    - Provide safeguards that can be adapted based on the results of the PIA.
7. **Complete the outsourcing procedure described in section 6.1 – step 6** to reflect the requirements for communicating data outside Québec.

7. Cybersecurity, incident management and biometrics

The new regime strengthens the obligation of organizations to protect personal information with new safeguards, renders confidentiality incident reporting obligations mandatory and amends the biometrics provisions of the *Act to establish a legal framework for information technology*.

7.1. Cybersecurity

Effective September 22, 2023

Security safeguards. The security requirements of section 10 of the Private Sector Act remain unchanged. As a reminder, organizations must take appropriate and reasonable security measures to protect personal information, taking into account, among other things, the sensitivity of the information, the purpose for which it is to be used, and the amount, distribution and medium of the information. Thus, the more sensitive the information, the stronger the safeguards must be. Security measures include technical, physical and organizational controls and should always be assessed and predefined according to the circumstances of each project, by conducting a technical security risk analysis in parallel with the privacy impact assessment. This ensures that the required arrangements are in place prior to signing the contract, taking into account the results of both assessments, which will greatly influence the legal recommendations and the negotiation of contractual clauses. The security risk analysis should always include due diligence on the vendor's security posture and the solution or service being offered, if applicable.

Protection measures. As part of the amendments to the Private Sector Act with respect to PIAs, the Privacy Officer may suggest, at any stage of a project, "measures to protect the personal information" as discussed in section 2.3. These "measures" must be interpreted as an addition to the general requirement to implement appropriate security measures as set out in section 10 of the Private Sector Act. In any event, the Privacy Officer should work with a security expert on an ongoing basis to ensure consistency in the identification and implementation of protection measures.

Security Freeze. The "security freeze" is one of the measures for protecting the personal information contained in the files of credit assessment agents, provided for in the *Credit Assessment Agents Act*. According to this Act, the security freeze prohibits the credit evaluation agent who holds the file that is the subject of the freeze from communicating the personal information contained in the file as well as the personal information produced from the file, when this communication is for the purpose of concluding a credit contract, increasing the credit granted under such a contract or concluding a long-term rental agreement for goods or a contract for the successive performance of a service provided at a distance.

Section 8.4 introduced by Bill 64 adds that when a person is notified of a security freeze of a file held by an agent, he or she may not request access to it from another credit assessment agent. Thus, in addition to the prohibition against disclosure by agents, there is a prohibition against disclosure to another agent.

Steps to compliance

1. **Categorize the information assets to assign security measures that correspond to the level of categorization.**
   - In particular, categorization levels should take into account the sensitivity of personal information, as well as the confidentiality, integrity, and availability requirements.
2. **Establish a collaboration system between the Privacy Officer and the security department so that the safeguards and protection measures are effective and consistent from one project to another.**
   - If necessary, form a privacy committee that includes the Privacy Officer, the IT/security departments and IT governance.
3. **If applicable, update your procedures to ensure the staff does not contact credit assessments agents if a security freeze has been placed on a file under the *Credit Assessment Agents Act*.**

7.2. Confidentiality incidents

In force September 22, 2022

Since September 2022, Québec has become the third jurisdiction in Canada, along with the federal jurisdiction and Alberta, to have a mandatory private-sector confidentiality incident reporting regime for incidents that present a risk of serious injury.

New section 3.6 defines a “confidentiality incident” as an unauthorized access, use, disclosure, loss or any other violation of the protection of personal information. The definition being rather broad, any breach, violation or incident involving personal information will fall under the application of section 3.6. Some of the different types of confidentiality incidents may include phishing, malware deployment, ransomware attacks, botnets, brute force attacks, sending personal information to the wrong email address, etc.

It is interesting to note that Québec is the only jurisdiction in Canada to include the unauthorized use of personal information in its definition of confidentiality incident. This inclusion could lead to uncertainties as to whether the use of personal information without consent for marketing purposes, for example, could be considered a “confidentiality incident”. While such an interpretation could lead to an overabundance of incident notifications to the CAI and to the individuals involved, companies will need to exercise judgment in assessing the risk of injury, as explained in the following sections.

Risk of serious injury assessment. All confidentiality incidents will be subject to a "risk of serious injury" assessment process to determine whether the incident in question should be notified to the CAI and the individuals involved. The notion of "risk of serious injury" proposed by the Québec legislator is subtly distinguished from the notion of "real risk of significant harm" provided for in PIPEDA and Alberta's PIPA, as the word "real" has been omitted. In addition, unlike PIPEDA, Bill 64 does not provide examples of serious injury, but does set out the following key factors to be considered in assessing the level of seriousness of the risk of injury:

(i) **The sensitivity of the information involved.** Information that, because of its nature (e.g., medical, biometric or otherwise intimate) or the context of its use, entails a high level of reasonable expectation of privacy will increase the risk of injury;

(ii) **The anticipated consequences of its use.** For example, whether the compromised information is likely to be used to commit fraud or identity theft;

(iii) **The likelihood that it will be used for injurious purposes.** If, for example, the information has been exfiltrated from the organization's servers or published on the Dark Web, it is likely to be used for injurious purposes.

Although the assessment criteria for PIPEDA and PIPA are superficially similar to Bill 64 test, we do not rule out the possibility that the CAI will interpret the notification requirements more narrowly, since the risk of serious injury does not have to be real for the notification obligation to be triggered. In any event, the Privacy Officer should be consulted in making this assessment (section 3.7 *in fine*).

Notification of incidents. If the organization determines that the incident poses a risk of serious injury, it will be required to notify the CAI and any individual affected by the incident, failing which the CAI may order the organization to do so. It is also provided that the organization may, at its discretion, notify any person or organization that may be able to reduce the risk of injury, but with only the personal information necessary to do so (without the consent of the individual concerned). In the latter case, the Privacy Officer shall record the disclosure. There is no time limit for reporting incidents, but reporting must be done "promptly", according to section 3.5. By comparison, PIPEDA and PIPA require notification as soon as possible to the OPC in the event that a breach of security measures presents a "real risk of significant injury". In Europe, the GDPR requires disclosure of a breach to the country's supervisory authority no later than 72 hours after the breach when it poses a risk of injury.

If a confidentiality incident occurs at a third party service provider or subcontractor to whom personal information has been outsourced, there may be contractual requirements for notification of incidents. However, since the new notification obligations of Bill 64 apply to any organization regardless of their role in the processing of personal information, a service provider or subcontractor may be required to report the incident since reporting the obligation applies to "any person carrying on an enterprise who has cause to believe that a confidentiality incident involving personal information the person holds has occurred." At the federal level, PIPEDA requires an organization to report a breach involving personal information under its control. It is unclear if the Québec legislator voluntarily omitted to mention the notion of control and whether the CAI would expect both the organization acting as the data controller and its service provider (and subcontractor) to report the incident which may require some type of coordination between these organizations.

Notwithstanding the foregoing, it should be noted that an individual affected by a confidentiality incident does not have to be notified if such notification would impede an investigation by a person or body that, by law, is responsible for preventing, detecting or suppressing crime or offences under section 3.5.

Notices to the CAI. Under the *Regulation respecting confidentiality incidents*, the following information shall be reported to CAI promptly when the organization becomes aware that a confidentiality incident present a risk of serious injury:

1. the name of the organization affected by the confidentiality incident and any Québec business number assigned to such organization under the *Act respecting the legal publicity of enterprises* (chapter P-44.1);
2. the name and contact information of the person to be contacted within that organization with regard to the incident;
3. a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;
4. a brief description of the circumstances of the incident and what caused it, if known;
5. the date or time period when the incident occurred or, if that is not known, the approximate time period;
6. the date or time period when the organization became aware of the incident;
7. the number of persons concerned by the incident and the number of those who reside in Québec or, if that is not known, the approximate numbers;
8. a description of the elements that led the organization 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;
9. the measures the organization has taken or intends to take to notify the persons whose personal information is concerned by the incident, pursuant to the second paragraph of section 63.8 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* or the second paragraph of section 3.5 of the *Act respecting the protection of personal information in the private sector*, and the date on which such persons were notified, or the expected time limit for the notification;
10. the measures the organization has taken or intends to take after the incident occurred, including those aimed at reducing the risk of injury or mitigating any such injury and those aimed at preventing new incidents of the same nature, and the date on which the measures were taken or the expected time limit for taking the measures; and
11. if applicable, an indication that a person or body outside Québec that exercises similar functions to those of the Commission d'accès à l'information with respect to overseeing the protection of personal information has been notified of the incident.

Please note that the CAI has published a report form on its website (available in French only). This form seems to require more information than what is required under the *Regulation respecting confidentiality incidents*.

Notices to the persons concerned. The notification to individuals affected by a risk of serious harm as a result of a confidentiality incident shall contain:

1. a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;
2. a brief description of the circumstances of the incident;
3. the date or time period when the incident occurred or, if that is not known, the approximate time period;
4. a brief description of the measures the organization has taken or intends to take after the incident occurred in order to reduce the risks of injury;
5. the measures that the organization suggests the person concerned take in order to reduce the risk of injury or mitigate any such injury; and
6. the contact information where the person concerned may obtain more information about the incident.

Mitigation of risk. Section 3.5 requires businesses that have "cause to believe" that a confidentiality incident has occurred to take "reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature". This requirement applies to any entity or third party that has custody or control of personal information, such as a service provider or subcontractor. In practice, this means that organizations will need to take all appropriate and reasonable steps to prevent injury to individuals as a result of the incident, and this, even if the incident does not pose a serious risk of injury. The steps to be taken will depend on the type of incident and the applicable context, but could include, for example, thorough investigations and any security measures to contain and eradicate the incident. We note that this obligation applies regardless of the seriousness of the risk.

A proper way to mitigate the risk of injury is to have a robust security program based on industry best practices, and to have the organization's incident response plan tested by incident response experts.

Register of confidentiality incidents. Organizations must keep a register of confidentiality incidents, which must contain the following information:

1. a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;
2. a brief description of the circumstances of the incident;
3. the date or time period when the incident occurred or, if that is not known, the approximate time period;
4. the date or time period when the organization became aware of the incident;
5. the number of persons concerned by the incident and the number of those who reside in Québec or, if that is not known, the approximate numbers;
6. a description of the elements that led the organization 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;

7. if the incident presents a risk of serious injury, the dates on which notices were given to the Commission d'accès à l'information and to the individuals concerned, as well as a statement indicating whether public notices were given by the organization and the reason for them, if applicable
8. a brief description of the measures taken by the organization following the incident in order to reduce the risk of injury being caused.

The information contained in the register shall be kept up to date and retained for a period of at least five years after the date or period in which the organization became aware of the incident.

Powers of the CAI. The CAI has power to issue several types of orders in relation to confidentiality incidents. In particular, it can order any person to apply the measures deemed appropriate to protect the rights of the persons concerned.

Steps to compliance

1. **Define an organizational structure with clear roles and responsibilities for incident prevention, management and response.**
   - Responsibilities should be detailed and clear according to the roles.
2. **Prepare or update the organization's incident management policy to include new obligations, and**
   - Develop a detailed incident response plan based on industry standards;
   - Have this plan tested and approved by incident response experts.
3. **Revise contracts with service providers to include the new incident notification** obligations to ensure that:
   - All incidents involving personal information are communicated to the organization promptly;
   - The provisions adequately reflect the new definition of "confidentiality incident";
   - Service providers are able to provide all the information required to allow the organization to assess the risk of serious injury.
4. **Define a training program for incident prevention and management.**
5. **Keep a record within the organization of all confidentiality incidents, even if they do not involve a risk of serious injury.** This log should include, at a minimum:
   - The person responsible for the investigation;
   - The circumstances of the incident;
   - The date or period of the incident;
   - The nature of the personal information affected by the incident, if known;
   - The reason why the company believes that the incident does not involve serious injury to the individuals involved.

7.3. Biometrics

In force September 22, 2022

Biometrics (which literally means "measurement of the human body" in Greek) is the practice of mathematically analyzing the biological, morphological, or behavioral characteristics of a person. When biometrics is discussed in the context of the IT Act, it is in reference to systems deployed to identify or confirm a person's identity using their biometric data, such as fingerprints, iris or retina structure, hand or facial geometry, or voice. This is an important distinction, as biometric data is considered sensitive personal information and is subject to privacy laws applicable to both the public and private sectors, regardless of the purpose for which it is used.

Identification and authentication are the main functions of biometrics. Each of these functions has its own technical components, thus generating distinct legal risks. While "identification" means finding an identity in a database to determine who a certain person is, "authentication" means verifying or confirming the identity of that person. For example, identification can be used to grant or deny access (i.e., the presence of captured biometrics has been confirmed in the database), whereas authentication is more about verifying or confirming that the individual is who they say they are. The identification function generally raises more technical and legal risks since a biometric database must be set up, which is not necessarily the case for the authentication function...

In 2001, the Québec legislator introduced, with the IT Act, a number of provisions aimed at regulating the use of biometric databases in order to ensure that the information contained therein benefited from an adequate level of protection. Bill 64 introduces changes to sections 44 and 45 of the IT Act, particularly concerning the obligation to declare the use of biometric technologies to the CAI. Prior to Bill 64, the disclosure requirement was limited to a "database of biometric characteristics and measurements" (in other words, biometric databases). Now, in addition to the existing requirement to obtain the express consent of individuals for the collection of their biometric data as provided for in section 44, Bill 64 adds the obligation to have previously declared to the CAI the use of a biometric system for the verification or confirmation of identity, even if no biometric data is stored in a database. Thus, without such a declaration to the CAI and express consent, an organization will not be permitted to use biometric technologies for the purposes mentioned above. This new requirement is consistent with the CAI's recommendations regarding Bill 64 in its document entitled "Brief of the *Commission d'accès à l'information* presented to the *Commission des institutions* in the context of specific consultations and public hearings." The CAI has published on its website a form to declare the use of a biometric system (only available in French). Please note that the same form is used to declare a biometric system and a database of biometric characteristics and measurements.

It should be noted here that a linguistic discrepency between the English and French versions of section 44 may lead to two completely different interpretations of this new obligation. While the French version provides that "Nul ne peut exiger, sans l'avoir divulgué préalable à la Commission d'accès à l'information et sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques", the English version reads as follows: "A person's identity may not be verified

or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the person concerned." Accordingly, the French version is interpreted *a contrario* as necessarily *requiring* the use of biometrics for the obligation to declare the system to apply. Since it is not possible in Quebec to require such an initiative, the amendment to section 44 may simply not apply. Alternatively, it is likely that the CAI will rely on the English version of section 44 and require any organization processing biometric data to declare it, even if the organization does not *require* it.

To conclude, it should also be noted that section 45 of the IT Act has been amended to require organizations to notify the CAI of the creation of any biometric database no later than 60 days before it is put into service. The Private Sector Act thus specifies a maximum period in which this notification must occur.

Steps to compliance

1. **Establish guidelines on the use of biometric systems** to include the above obligations and on the protection of biometric data.
2. **Conduct a privacy impact assessment** prior to any project involving biometric data.

This Guide will be updated by the BLG (Montreal) Privacy and Data Protection Team on a regular basis to reflect regulatory developments and relevant guidance published by the CAI and other stakeholders.

Key Contacts

For any questions you may have about recent developments regarding the legal framework governing data protection in Québec, please reach out to a member of BLG's Cybersecurity, Privacy & Data Protection team:

Katherine Poirier
Partner
T 514.954.3175
kpoirier@blg.com

Frédéric Wilson
Counsel
T 514.954.2509
fwilson@blg.com

Patrick Laverty-Lavoie
Senior Associate
T 514.395.3887
plavertylavoie@blg.com

Candice Hévin
Senior Associate
T 514.954.2588
chevin@blg.com

Simon Du Perron
Associate
T 514.954.2542
sduperron@blg.com