Borden Ladner Gervais

Act respecting the protection of personal information in the private sector:

Compliance guide for organizations

February 2026

Act respecting the protection of personal information in the private sector:

Compliance guide for organizations

This Guide is intended to help organizations comply with the requirements of the *Act respecting the protection of personal information in the private sector* ("**Private Sector Act**").

The Guide is divided into different topics that reflect the key obligations under the Private Sector Act – the private sector privacy regime. It is designed for any person who collects, holds, uses or communicates personal information in the course of carrying on an enterprise.

Best Practices

Under each topic, we outline some suggested measures that organizations can adopt to strengthen their compliance and demonstrate proactivity in protecting personal information.

Table of Contents

This Guide is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this Guide. No part of this Guide may be reproduced without prior written permission of Borden Ladner Gervais LLP.

1. Enforcement mechanisms

The Private Sector Act sets out three types of mechanisms to ensure that organizations comply with personal information processing requirements, namely (1) administrative monetary penalties, (2) penal offences, and (3) a private right of action.

Administrative Monetary Penalties The Private Sector Act provides for a system of administrative monetary penalties ("**AMPs**") administered by the Commission d'accès à l'information ("**CAI**"). Under its provisions, a "person designated by the Commission, but who is not a member of any of its divisions" may impose AMPs on organizations that contravene the law (see Table 1.1 for specific offences) of up to $10,000,000 or 2% of worldwide turnover.

According to the CAI's General Framework for the Application of Administrative Monetary Penalties ("**AMP Enforcement Framework**") (available in French only), the person responsible for imposing AMPs has been designated by the CAI as the director of the Oversight Division or, in their absence, the person acting in that capacity. This person has discretionary power to assess whether a penalty should be imposed, taking into account all the circumstances specific to each case. A sanction is generally imposed when a violation provided for in section 90.1 of the Private Sector Act is observed and the criteria set out in the AMP Enforcement Framework are met (see Table 1.3 for a list of criteria).

Before imposing an AMP, the CAI issues a notice of non-compliance, inviting the organization to remedy the situation. If no correction is made, the sanction is then formalized through a notice of claim setting out the amount owed, the reasons for it, the applicable deadlines, and the possible recourses — including the right to apply for a review of the decision or to contest the review decision before the Court of Québec. It is also possible to enter into a formal undertaking with the CAI to correct the violation and avoid a sanction.

Penal offences The Private Sector Act provides for several offences (see Table 1.1 for the specific offences) for 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.

According to the AMP Enforcement Framework, the CAI generally prioritizes penal proceedings when this avenue is deemed the most appropriate in light of the objectives pursued and the circumstances of each case. Penal proceedings are notably considered in the following situations:

- The consequences of the offence are serious, particularly in cases involving an invasion of privacy, an impact on a vulnerable clientele, or a compromise of sensitive information;
- Failure to comply with an order issued by the CAI;

- The offender has not taken the appropriate measures to remedy the offence, despite the imposition of AMPs or the use of other administrative measures;
- The offender acted intentionally or demonstrated negligence or recklessness;
- Obstruction of a CAI investigation or inspection has been observed;
- Obstruction of the processing of a CAI request has been observed, including by providing false or inaccurate information or by failing to provide required information;
- Multiple violations or offences under the Private Sector Act have been committed by the same offender, or are recurrent over time.

The decision to initiate penal proceedings is made by a member of the CAI's Oversight Division and is commenced by serving a statement of offence.

Punitive Damages The Private Sector Act recognizes the possibility for individuals to claim punitive damages of at least $1,000 when an unlawful infringement of a right conferred by the Private Sector Act or by articles 35 to 40 of the Civil Code of Québec ("**CCQ**") causes an injury, provided the infringement is intentional or results from gross negligence. Section 93.1 of the Private Sector Act constitutes a provision for the award of punitive damages within the meaning of article 1621 of the Civil Code.

It should be noted that, as of January 1, 2026, no AMPs or penal sanctions have been imposed. That being said, we are seeing an increase in the number of proceedings in which plaintiffs are claiming punitive damages, including Synotte v. TikTok Technology Canada Inc. (2025) (available in French only) and S.C. v. Gameloft et al. (2025) (available in French only). It will be important to monitor these cases closely to see whether such damages will be awarded.

The following tables provide a summary of the enforcement mechanisms provided by 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	X	X	X
Failure to inform the individuals in accordance with sections 7 and 8 at the time of collection		X	X
Failure to take appropriate security measures necessary to ensure the protection of personal information pursuant to section 10	X	X	X
Failure to notify the CAI or the individuals concerned of a confidentiality incident that presents a risk of serious injury	X	X	X
Failure to inform the individual affected by a decision based on an automated processing of personal information or provide an opportunity submit observations		X	X
Identify or attempt to identify an individual using de-identified or anonymized information without the authorization of the organization who holds the information	X		X
Impede the progress of an investigation, an inspection or the hearing of an application by the CAI	X		
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	X		X
Failure to comply with a request for production of documents issued by CAI within the specified time	X		
Failure to comply with an order from the CAI	X		

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	Director of the CAI's Oversight Division	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)

* 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 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, 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 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

The Private Sector Act formally recognizes that every organization is responsible for the protection of personal information it holds. This principle gives rise to a number of accountability and data governance obligations.

2.1. Privacy Officer

Designation. The Private Sector Act 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 law. However, this role of "Privacy Officer" may be delegated in writing, in whole or in part, to any person. This can be a member of the personnel of the organization or a third party. According to the CAI's guidance (available in French only), even in cases of delegation, the highest authority within the organization remains ultimately accountable for compliance with the Private Sector Act. The organization must ensure that the title and contact details of its Privacy Officer are available on its website or, if that is not possible, through any other appropriate means.

Duties. The Privacy Officer may be called upon to perform various functions, which may include the following tasks:

- Approve governance policies and practices regarding the protection of personal information that the organization must adopt and implement, and ensure internal training for their implementation. See section 2.2 below for more details on these policies and practices.
- Participate in the conduct of Privacy Impact Assessments ("**PIAs**") for acquisition, development and overhaul projects involving certain information systems or electronic service delivery systems and suggest measures to ensure the protection of personal information processed in connection with such systems. See section 2.3 below for more details on PIAs.
- Take part in the management of confidentiality incidents, including by assessing the injury caused, and record any communication (without consent) to another organization or public body that may mitigate such injury, and act as the point of contact for communications with the CAI. 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 de-indexation. See section 5 for more details on new individual rights.

Qualifications. The Private Sector Act 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 can therefore 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. It may also retain the services of lawyers specialized in privacy and personal information protection to assist the Privacy Officer in carrying out their duties.

Best Practices

1. **Determine the qualifications required to fulfill the role of Privacy Officer.**
   Organizations should determine whether they have the necessary expertise in-house, 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 the Private Sector Act and the reality of the organization.
3. **Designate an individual as the Privacy Officer in writing.**
   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

Policies and practices. The Private Sector Act formally recognizes the duty of organizations to establish and implement governance policies and practices relating to the protection of personal information. 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 personal 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, or by any other appropriate means, in clear and simple terms. Although the level of detail is not defined, the objective is to present the organization's practices in an accessible manner, including the information mentioned above.

Organizations can incorporate this information into a 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, or information on the organization's security certifications.

Content. Unlike the Act respecting Access to documents held by public bodies and the protection of personal information — which is supplemented by a Regulation specifying the mandatory content of public bodies' privacy policies — the Private Sector Act contains no such requirements for enterprises. However, according to the CAI's Explanatory Guide (available in French only), policies may include:

- The name of the organization, the effective date of the policy and the date of its most recent update;
- The means by which the personal information is collected through technological means, the use of identification, location or profiling technologies, and how such functions may be activated (if applicable);
- The identity of the entities collecting personal information for the organization;
- The categories of personal information collected and the specific purposes for which it is collected;
- The measures available to individuals to refuse the collection of certain personal information and the consequences of such refusal;
- The categories of individuals within the organization who have access to personal information;
- Where disclosure to third parties occurs: the information or categories of information involved, the purposes of such disclosures, the names or categories of recipients, and an indication of any transfers outside Québec (if applicable);
- The rights of individuals, including the right of access, rectification, updating, and the ability to file a complaint with the organization in accordance with the established process.

Best Practices

1. **Conduct an inventory and regularly update the policies and procedures in place to protect personal information throughout its life cycle.**
2. **Regularly conduct a data mapping exercise to document and update the organization's personal information management practices.**
3. **Ensure the following policies and procedures are implemented, (or incorporate them into an "internal privacy framework"), depending on the organization's needs and activities:**
   - 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 outlining the roles and responsibilities of staff members throughout the life cycle of personal information.
   - 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.
   - Vendor risk assessment policy.
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, as well as their updates**
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) or by any other appropriate means.**

2.3. Privacy Impact Assessments ("PIAs")

Requirement to conduct a PIA. Organizations are 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. The Private Sector Act also provides for two other situations in which a PIA is mandatory for organizations: (1) the communication of personal information outside Québec, and (2) the communication of such information, without the consent of the individuals concerned, for study or research purposes or for the production of statistics under an agreement.

According to the Office québécois de la langue française ("**OQLF**"), an information system consists of human resources (personnel), material resources (equipment), and the procedures used to acquire, store, process, and disseminate information elements relevant to the operation of an organization (e.g., databases, application software, procedures, documentation, etc.). It is important to distinguish an information system from an information technology system. The latter refers only to the technological component of the information system, such as the central processing unit, peripherals, operating system, etc. Electronic service delivery is defined as "the delivery of government services, whether secure or not, offered to citizens over the Internet."

Examples of projects covered by the requirement. The CAI has published a Guide on conducting PIAs which was updated in April 2024. In this guide, the CAI provides recommendations to organizations on how to carry out a PIA for any project involving personal information. According to the CAI, projects that require a PIA include, in particular, those that aim to:

- Offer a new public service;
- Deploy an existing service on the Web;
- Increase the security of a facility;
- Combat fraud;
- Improve the detection of a rare health condition;
- Ensure regulatory compliance;
- Maintain your competitiveness;
- Provide a more user-friendly customer experience by creating a new version of a platform.

Not retroactive. The requirement to conduct a PIA is not retroactive. Thus, organizations do not have to assess existing systems prior to the entry into force of the relevant provisions of the Private Sector Act, that is, before September 22, 2023. However, the substantial update of an existing system (e.g., a document-management platform) should be considered a "redesign" and must therefore be subject to a PIA, including in situations where a PIA has already been completed.

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". It should be noted that the same criteria as those under section 10 of the Private Sector Act are used to determine the types of security measures that an organization must implement to protect the personal information it holds. This requirement is 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 seeking to familiarize themselves with the process, which must be initiated at the very beginning of the project. The CAI has also published a PIA Report Template (available in French only) to support organizations in this process.

Data portability. In addition, organizations 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. See section 4.3 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, using for example of the CAI's PIA Report Template (available in French only).**
   - 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

Highest level of confidentiality. The Private Sector Act 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. However, browser cookies are expressly exempt from this requirement.

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 the Private Sector Act, 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.

Best Practices

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 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

The Private Sector Act establishes transparency and consent rules.

3.1. Transparency and obligation to inform prior to consent

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.

Obligation of transparency. TIn its Guidelines on the Validity of Consent (the “Consent Guidelines”) and in the joint investigation of TikTok (2025), the CAI clearly states that transparency is by default the legal basis for collecting personal information. This approach is specific to Québec and differs from other Canadian or international privacy laws, which regulate the collection of personal information primarily through consent.

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: (1) the purposes for which the information is collected; (2) of the means by which the information is collected; (3) the rights of access and rectification provided by law; (4) their right to withdraw consent to the communication or use of the information collected; and if applicable, (5) of the name of the third person for whom the information is being collected; (6) 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 (7) the possibility that the information could be communicated outside Québec).
- **On request.** An organization must also inform, on request, the individual of: (1) the personal information collected from them, (2) the categories of employees who have access to the information within the organization, (3) the duration of the period of time the information will be kept; and (4) the contact information of the Privacy Officer. When collecting information from another organization, an organization must, at the request of the individual, inform them of the source of the information, 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. 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". As such, this 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 CAI's interpretation of section 8.1 confirms that the use of this type of technology must be expressly permitted by individuals. Indeed, in its Consent Guidelines, the CAI states that such technologies must be deactivated by default. In all cases, in light of the CAI's interpretation, it is necessary to consider revisiting the use of certain technologies intended to profile, track, or identify individuals, and to implement processes that require the user to activate certain functions. One example is consent banners for the use of cookies; users must be informed about the use of cookies and how to activate certain features, such as profiling

- **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. 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. See section 2.2 for more details on the content of privacy policies.

  Other Canadian privacy laws grant individuals a similar right to obtain information about the processing of their personal information. However, this right falls within the broader right of access, meaning that when an organization receives such a request, it must process it in accordance with the procedure and timelines applicable to an access request. By contrast, the Private Sector Act separates these two rights, thereby creating a more flexible framework for requests made under the above-mentioned provisions. Nonetheless, it is recommended to act diligently, as failing to inform individuals in accordance with these provisions is expressly listed among the situations that give rise to the imposition of AMPs (see section 1).

- **Automated decision-making.** The Private Sector Act also imposes transparency requirements for an organization using personal information to render a decision based exclusively on automated processing of such information. See section 3.4 for details on these requirements.

Best Practices

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 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 another organization (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

The Private Sector Act sets out the rules regarding the form of consent, the criteria that must be fulfilled in order to ensure the validity of consent, and the requirements for obtaining consent from minors. It also establishes a necessity criterion for the collection.

Necessity criterion. The Private Sector Act requires that any organization intending to collect personal information first identify a serious, legitimate, and specific purpose for the collection. Once this purpose has been established, the organization may collect only the personal information that is strictly necessary to achieve that purpose. The necessity criterion is not optional: it applies in all circumstances, regardless of whether consent has been obtained. It is also important to note that this necessity requirement applies at every stage of the personal information life cycle, not only at the time consent is obtained. According to the CAI's guidance (available in French only), a collection is considered necessary only if all the following conditions are met:

- The purpose pursued is legitimate, real, and important;
- The collection is rationally linked to that purpose;
- There are no less intrusive means to achieve the same result; and
- The benefit of the collection for the organization outweighs any potential injury to the individual concerned.

Thus, according to the CAI's decisions in Imprimeries Transcontinental Inc. (2024) ("T**ranscontinental Decision**") and 13859380 Canada Inc. (Crane Supply) (2025) ("**Crane Supply Decision**") (both available in French only), organizations collecting personal information must demonstrate the necessity of the collection by showing:

1) The "legitimate, important, and real nature of the objective pursued through the collection"; and

2) The "proportionality of the privacy breach that the collection represents in relation to the objectives pursued".

(Our translation)

As part of the first criterion, the CAI held in the Transcontinental Decision that, to establish the real nature of the objective pursued by an organization, the organization must demonstrate that the objective "is supported by specific events or issues that justify the necessity of collecting personal information, and not merely hypothetical considerations."(Our translation)

As for the second criterion concerning the proportionality of the intrusion, the CAI states in the Crane Supply Decision that the analysis must determine three elements:

- **The use is rationally connected to each objective**. Is the collection an effective means of achieving the stated objectives?
- **The intrusion is minimized**. Could the organization have used other, less intrusive means to achieve the intended objectives?
- **The information collected is clearly more useful to the organization than harmful to individuals**. What is the individuals' reasonable expectation of privacy?

If these conditions are not met, the collection must not be carried out and, in case of doubt, the information is presumed unnecessary. According to the CAI's guidance (available in French only), necessity must be assessed with respect to each intended purpose, and it is the organization's responsibility to demonstrate it. As a general rule, refusing to provide such information cannot be used as grounds to deny a product, service, or employment, unless the collection is necessary for entering into or performing a contract, is authorized by law, or there are reasonable grounds to believe that the request is unlawful.

Form of consent. With respect to the form of consent, the CAI recognizes that consent is obtained once the transparency obligation is met and individuals provide their personal information. In our view, this resembles a form of exchange of wills, whereby the act of agreeing to provide one's personal information constitutes a manifestation of the will to be bound. In this sense, one could say that consent is presumed. That being said, the Private Sector Act 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.

Thus, under the Private Sector Act, consent may be express, implied or presumed. However, implied or presumed consent is permitted, according to the Consent Guidelines, only if the following criteria are met:

- The use or disclosure does not conflict with the reasonable expectations of individuals in the circumstances; and
- No risk of serious injury arises from the intended use or disclosure.

Some have taken the position that there is uncertainty regarding how these provisions should be interpreted, and specifically, whether express consent must be obtained for the collection of sensitive personal information, even when the organization has properly described the purposes of the collection in its privacy policy, since no distinction is made between sensitive and non-sensitive personal information in section 8.3. Insofar as the criteria set out in sections 8 and 8.3 are met, we consider that nothing prevents the use of implied consent. 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. That said, the general practice is to obtain express consent for secondary purposes when the collection involves sensitive personal information, due not only to the nature of such information but also to the risk of sanctions for non-compliance with the Private Sector Act (see section 1 for more information on sanctions).

The CAI also distinguishes between consent for so-called "primary" purposes and "secondary" purposes:

- Primary purposes: "refers to the purposes for which personal information is collected by an organization. These purposes relate to the provision of a service or product, or access to employment. They are disclosed at the time of collection."
- Secondary purposes: "refers to all other purposes pursued by an organization."

In its Consent Guidelines, the CAI states that consent for primary purposes may be presumed as long as individuals have duly received the information required by law (see section 2.2). In all cases, the collection, use, or disclosure of personal information for either primary or secondary purposes must be supported by valid consent. It should be noted that there is some uncertainty regarding the exact definition of "secondary purposes," which may refer to purposes that were not disclosed at the time of collection or purposes that are not essential to the contract or service offered by the organization.

Validity of consent. The Consent Guidelines provide clarification on the criteria for valid consent under the Private Sector Act. In particular, the CAI specifies that, in order to obtain valid consent, organizations must meet the following criteria:

- **Consent must be clear**. The CAI interprets clear consent as consent that is obvious and provided in a way that clearly demonstrates the individual's true will.
- Consent must be free. Freedom of choice or consent implies that the individual has a genuine ability to choose and real control. The exercise of choice must not be unduly influenced, and the person must not suffer disproportionate injury. It should also be noted that the CAI indicates that refusing to consent must be just as simple as giving it. In other words, options must be presented fairly; otherwise, consent may be considered invalid. Furthermore, the CAI reiterates that an organization cannot require the collection of personal information as a condition of service unless such collection is essential to providing the product or granting access to employment (i.e., for primary purposes). To this end, organizations must allow individuals to refuse the collection of their personal information for secondary purposes (as defined above). If the purposes for collection change, the organization may be required to obtain consent again.
- **Consent must be informed**. The individual must understand what they are consenting to and what it entails. According to the CAI, informed consent must be not only specific but based on appropriate knowledge. The individual giving consent must be capable of consenting—that is, must be at least 14 years old and not incapacitated. Consent given by authorized representatives is considered valid under the Consent Guidelines. The information listed in section 8 of the Private Sector Act enables the provision of informed consent (see section 2.2 for more information on privacy policies).
- **Consent must be given for specific purposes**. This principle is closely tied to informed consent. The CAI interprets it as requiring a precise and clearly defined object—meaning that the purpose(s) for the use or disclosure of personal information must be described as specifically as possible. The terms used to define these purposes must be appropriate and cannot be vague, broad, or imprecise. Consent is therefore restrictive, and any new purpose requires new consent.

- **Consent must be granular**. The Private Sector Act requires that consent be requested for each specific purpose. Under the Consent Guidelines, this principle ensures that consent is genuinely free, as it allows individuals to clearly indicate their agreement or disagreement with each purpose.
- **The request for consent must be comprehensible**. The Private Sector Act requires that the request for consent be made in simple and clear terms. According to the Consent Guidelines, the goal of this requirement is to guarantee informed and specific consent.
- **Consent must be temporary**. Under the Private Sector Act, consent is valid only for the period necessary to achieve the purposes for which it was sought. According to the CAI, the temporary nature of consent may be assessed either based on a time period (e.g., a number of days or months) or an event (e.g., completion of a payment).
- **The request for consent must be presented separately**. The Private Sector Act requires that written consent requests be presented separately from any other information. As such, the Consent Guidelines specify that the request must be distinct (e.g., separate from terms of use, privacy policies, signatures, etc.).

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. 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.

Best Practices

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.

→ Continued on next page

Best Practices

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 and help them 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.
5. **Ensure diligent monitoring of the consents obtained to guarantee that clients' preferences are respected and that any changes to consent are implemented within the organization. This can be achieved, in particular, through the use of a consent management platform.**

3.3. Exceptions to the consent requirement

The Private Sector Act provides exceptions to consent, allowing the use or disclosure of personal information without consent in predetermined situations.

Use without consent. Under the Private Sector Act, 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 or necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures.
- **Interest of the individual.** When it is clearly used for the benefit of the individual.
- **Research, data analytics and AI.** When its use is necessary for study, research, or statistical purposes and the information has been de-identified, meaning it no longer allows a person to be directly identified (see below for more information on de-identification or section 6.2 regarding anonymization).
- **Consistent purposes.** When its use is for purposes that are consistent with those for which it was originally collected.

Communication without consent. Under the Private Sector Act, 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. See section 5.1 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. 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 below 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: (1) to use the information only for the purpose of completing the commercial transaction; (2) not to communicate the information without the individual's consent unless otherwise authorized by law; (3) to take the necessary measures to ensure the protection of the confidentiality of the information; and (4) to destroy the information if the commercial transaction is not completed or if its use is no longer necessary. 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.

Information relating to the performance of a business function. The Private Sector Act excludes "personal information concerning the performance of duties within an organization by the person concerned" from the scope of its divisions II and III (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". While this exclusion 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 (work email addresses) to send commercial messages remains subject to requirements under Canada's anti-spam legislation.

Employment relationships. It should be noted that the Private Sector Act does not introduce a consent exception for the collection, use or communication of personal information to establish, manage or terminate an employment relationship. However, 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. According to the Consent Guidelines, it is generally difficult to consider an employee's consent to be "freely" given in this context, because of the inherent power imbalance in the employment relationship. An employee may believe, correctly or incorrectly, that their employment would be jeopardized by a refusal to consent. Conversely, 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. The CAI therefore encourages organizations to adopt mitigation measures tailored to their context, including ensuring neutrality in consent requests, offering alternatives where possible, and providing enhanced transparency.

Consent exception for research. The Private Sector Act allows the disclosure of personal information for research purposes under certain conditions, including:

- Conducting a PIA which conclude that: (1) the personal information is needed to achieve the research objective; (2) it is unreasonable to require the requesting person or body to obtain consent from the individual concerned; (3) the objective of the research outweighs the impact on individual privacy in light of the public interest; (4) the information is used in a manner that ensures its confidentiality; and (5) only the necessary information is communicated.
- A diligent review of the applicant organization's policies and practices. This is particularly important because, if the requesting person becomes the victim of a privacy incident compromising the disclosed information (see section 7.2 on privacy incidents), the disclosing organization may be subject to close scrutiny in the event of a CAI investigation.
- The conclusion of an agreement between the parties setting out, among other things, the terms of access, security measures, conditions for use, disclosure and retention, and the obligation to notify both the CAI and the disclosing organization in the event of a confidentiality incident or a breach of the agreement.
- A notice sent to the CAI containing the agreement between the parties, which will come into force 30 days after it is received by the CAI. While the Private Sector does not grant the CAI the power to terminate the agreement if it fails to fulfil all of the requirements, the CAI could nonetheless order the disclosing organization not to proceed until the agreement is revised to include the stipulated elements, suspend the agreement, or exercise its other oversight powers under the law.

Exception for internal research and analytics. The Private Sector Act allows organizations to use, without individuals' consent, the personal information they hold for the purposes of study, research, or the production of statistics, provided that the information has been de-identified. Since the consent exception in section 12 applies to the internal use of personal information within an organization, it is natural to interpret the terms "study" or "research" as encompassing business analytics. Indeed, by analogy with the definition of a "research project" found in the Act respecting health and social services information, business analytics also constitutes a structured process aimed at developing knowledge and innovation. This exception also extends to other forms of internal research activities, including those that rely on machine learning or other advanced data-analysis techniques that may be involved in the development of automated decision-making systems (discussed in more detail in section 3.4).

The Private Sector Act provides that personal information is "de-identified when it no longer allows the individual concerned to be directly identified." This definition essentially corresponds to the concept of "pseudonymization" as generally understood, including under the General Data Protection Regulation ("**GDPR**"). By comparison, the Private Sector Act also sets out criteria for the anonymization of personal information, specifying that information about an individual is anonymized when it can no longer, irreversibly, be used to identify that individual directly or indirectly (see section 6.2 for more information on anonymization).

It is worth noting that the wording of section 12 also clearly provides that no consent is required, even when the information is sensitive prior to anonymization.

In the Val-des-Cerfs (2022) decision, the CAI found that the data transmitted by the organization to its partner for algorithm development constituted de-identified personal information, not anonymized information, because the measures taken were not irreversible. The CAI concluded that the information contained in the database allowed the organization to identify students using other information collected throughout their academic career (e.g., indirect identification). It will be interesting to see how this reasoning evolves and whether it is adopted in future cases.

The Private Sector Act acknowledges the risk of re-identification associated with de-identified information by requiring organizations that use such information to take "reasonable measures to limit the risk of someone identifying a natural person using de-identified information." Furthermore, although not expressly stated, it would be consistent with the definition of sensitive personal information under the Private Sector Act (as well as CAI guidance and positions of other Canadian privacy commissioners) to interpret "reasonable measures" as requiring additional or more robust safeguards when the personal information underlying the de-identified information is sensitive. Unlike anonymized information, de-identified information remains personal information and is therefore still subject to the Private Sector Act.

It is important to note that internal research conducted under these provisions may require the completion of a PIA when it forms part of a project involving the acquisition, development, or overhaul of an information system or an electronic service delivery system (see section 2.3).

Best Practices

1. **Regularly 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 (and 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

Best Practices

3. **Implement a procedure to manage communications** of personal information in the context of a commercial transaction or research.
4. **Exercise caution when using the "consistent purposes"** exception to support the use of sensitive personal information in internal research. When the information is sensitive, the CAI may ask whether the use for a secondary purpose aligns with the individual's reasonable expectations, rather than asking whether such use is objectively consistent with the original purposes.
5. **Take the necessary measures to reduce the risk of re-identification** when the organization uses de-identified information under the exception for "study or research purposes," and adopt more stringent measures to prevent re-identification when the personal information underlying the de-identified information is sensitive.
6. **Implement a procedure to conduct a PIA** when the internal research falls within a "project involving the acquisition, development, or overhaul of an information system or electronic service delivery system".

3.4. Automated decision-making

The Private Sector Act 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, i.e. when there is no human in the loop. 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, or based on the use of a biometric system.

Notice and information requirements. The Private Sector Act 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. Organizations using technologies to make decisions based exclusively on automated processing should also indicate the use of such technologies in general terms in their privacy notices.

The Private Sector Act 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.

"Automated processing" is not defined under the Private Sector Act. Any forthcoming guidelines from the CAI will therefore be essential to delineate the scope of the requirements introduced in section 12.1. While the target of the amendments introduced by the Private Sector Act seems to focus on automated decision-making that has a significant effect on individual rights, with a focus on artificial intelligence ("**AI**") technologies, the wording of the section is broad enough that all sorts of other automated processes that make "decisions" could be caught up in its scope. In the absence of a clear definition, several organizations have chosen to limit its application to decisions that have a certain impact on individuals' rights and obligations (thus excluding, for example, targeted advertising).

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 set out, prior to the law's entry into force the Guidelines on Automated individual decision-making and Profiling for the purposes of the GDPR. We note that the interpretation formulated by the Working Party was facilitated by the restrictive wording of the GDPR provisions that target automated processing that "produces legal effects or similarly significantly affects the data subjet". The CNIL in France has also produced its own interpretation of the terms (available in French only). The Private Sector Act has 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 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, is 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 (1) disclose trade secrets or intellectual property of the organization or of third parties (such as service providers that provide the automated processing technology) or (2) enable fraudsters to game the system.

Individual right to submit observations. In addition, the concerned individual 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, the Private Sector Act 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) 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 organization does not seem to have a separate obligation to deliberate and come to an independent conclusion, or provide any reasons as to why a decision should be reviewed or not. 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.

Best Practices

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 Best Practices for section 4 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 concerning a decision based on an automated processing** 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.

4. Individual rights

Individuals are granted many rights under the Private Sector Act: a right of access to their personal information, a right to rectification, a right to control the dissemination of their personal information (also known as the "right to de-indexation"), a right to data portability, a right to be informed of, and submit observations on automated decision-making (see section 3.4), and a right to request further information from organizations about their data processing (see section 3.1).

4.1. Right of access and to rectification

Every individual has the right, under the Private Sector Act, to know whether an organization holds personal information about them and to have access to it. They may also request that the information be corrected when it is inaccurate, incomplete or equivocal, or when its collection, communication or retention is not authorized by law. The organization must then make the appropriate corrections and update the relevant records.

Access to personal information is free of charge, except for fees limited to the cost of transcription, reproduction or transmission, which must be announced in advance and set in accordance with the Regulation respecting fees.

Form of the request. An organization must consider only written requests submitted by a person who proves that they are indeed the individual concerned by the personal information, or by an authorized representative such as a holder of parental authority.

Delay to respond to the request. The Privacy Officer must respond in writing within 30 days of receiving the request. However, the organization may ask the CAI within that initial 30-day period to extend the response time. Unlike other Canadian privacy laws, no limit is set on the total number of days for which the CAI may grant an extension.

Refusing the request. When 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 (where applicable), and inform the requester of the remedies available to them and the applicable time limits. In this regard, the organization must inform the requester of their right to file an application for review of a disagreement with the CAI within 30 days following the refusal. Upon request, the Privacy Officer must also assist the requester in understanding the refusal.

Complete and diligent search. To ensure these rights are effectively upheld, the Privacy Officer must conduct a complete and diligent search for the personal information covered by any request made to the organization. To support this process, the CAI provides an Information Sheet (available in French only) outlining best practices at each step.

Restrictions on the right of access. The right of access is not absolute. Thus, the organization receiving an access request may refuse to disclose the information, notably when disclosure could

reveal the identity of a third party and seriously injury them without their consent, could affect ongoing judicial proceedings, or when the request is manifestly abusive.

4.2. Right to de-indexation

The Private Sector Act affords individuals the right to control the dissemination of their personal information by organizations and online intermediaries who facilitate the dissemination of such information, such as search engines, content publishers and online intermediaries (e.g., social media platforms). This right is more commonly known as the right to be de-indexed, 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 or causes serious harm to the reputation or privacy of an individual. Unlike the right to be forgotten found in the EU's GDPR, Québec's right to be de-indexed 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 provide under section 28 of the Private Sector Act and article 40 of the Civil Code, which set out three situations in which an individual may request that an organization delete personal information it holds about them: (1) when the information is outdated; (2) when retaining the information is no longer justified in light of the purpose for which it was collected; or (3) when the information was collected in a manner that does not comply with the law.

Scope of the right to be de-indexed. Under this 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 (1) contravenes the law or a court order, or (2) otherwise causes serious injury to the individual's reputation or privacy.

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, such as the public status of the individual, their age, the types of personal information disseminated, the context and the time elapsed since the publication.

Interestingly, this 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.

Format of the request. These types of requests follow exactly the same process as access and rectification requests. However, when such a request is granted, the Privacy Officer must respond in writing and provide a certification that the information is no longer being disseminated or that the hyperlink has been de-indexed or re-indexed, as applicable.

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 delisted 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.

4.3. Right to data portability

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". This information must also be communicated in the form of a written and intelligible transcript. For more information, see our article *Québec Law 25 still has more to say: Answers to your questions on the new data portability right*.

Meaning of "structured, commonly used and technological format". The terms "structured", "commonly used" and "technological" are not explicitly defined within the Private Sector Act, and their meaning is likely to vary depending on the industry or sector involved. According to the Québec Government's guidance (available in French only), open formats such as CSV, XML and JSON, accompanied by metadata useful to understanding its meaning, are adapted to the data portability right.

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 (see section 2.3 for more information about PIAs).

Format of the request. This type of request follows exactly the same process as access and rectification requests.

Exemptions to data portability. The right to data portability, like the right of access it complements, is not absolute. An organization that receives a request under this right may refuse to disclose the information for the following reasons:

- **In the event of serious practical difficulties.** 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. Such difficulties may arise, in particular, from the significant costs and/or the complexity involved in transferring the information into the appropriate format or to a third party. An organization invoking such grounds must be able to demonstrate these difficulties if the request is ever reviewed by the CAI.

- **If a restriction to the right of access applies.** Since portability is an extension of the right of access, the provisions that allow organizations to refuse access to certain information also apply. 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.
- **If the request is manifestly abusive.** Organizations may refuse portability when the requests are clearly unfounded or excessive, particularly due to their repetitive or systematic nature, or because they do not align with the purpose of the law, provided that authorization is obtained from the CAI.

Best Practices

1. **Prepare an inventory of practices that may trigger the application of 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 organization authorized by law to collect such information, in a structured, commonly used and technological format upon request.
3. **If the organization disseminates personal information or operates an online search tool, implement a procedure to guarantee that:**
   - The organization is able to receive, evaluate and respond to a right to be delisted 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.

5. Outsourcing and transfers outside of Québec

The Private Sector Act provides requirements for outsourcing and communicating of personal information outside Québec.

5.1. Outsourcing

Openness. As noted in section 3.1, the Private Sector Act 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 organization's privacy policy. This means that the organization's privacy notice has 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, the Private Sector Act 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. This exception therefore allows the organization to transmit personal information to its agents and service providers without the individual's consent, subject to specific contractual provisions between the organization and its service providers. We refer to the 'Written Agreement' paragraph below for the requirements applicable to data protection addendums.

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 is required to conduct a PIA. While this is the responsibility of the organization, service providers should cooperate in this exercise. We refer to section 2.3 for PIA requirements.

Written agreement. The Private Sector Act 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:

- **Protecting 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;
- **Only using information 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;
- **Not retaining the personal information after the contract expires;**

- **Notifying the Privacy Officer without delay of any breach or attempted breach** by any person of any of the obligations concerning the confidentiality of the information communicated; and
- **Allowing the Privacy Officer to conduct any audit related to these confidentiality obligations.**

Beyond what is required under the Private Sector Act, a written agreement of this nature includes, among other things, the following elements:

- Informing the organization of any request received from an individual concerning personal information or any right that may arise under Canadian privacy laws;
- Informing the organization of any disclosure request originating from a governmental or regulatory body and cooperating with that body; and
- Governing, restricting, or prohibiting transfers of personal information outside Québec or Canada.

Obligation to notify breaches of confidentiality obligations. The Private Sector Act also 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. The CAI has not yet clarified whether the parties may adjust the terms of the obligation where applicable, for example by limiting the notification obligation to "confidentiality incidents" only.

Authorizing 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. The CAI has not yet clarified whether the parties may adjust the terms of the obligation where applicable for example by requiring that audits occur only at certain times or under 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.

Best Practices

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).

→ Continued on next page

Best Practices

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;
   - The requirement by the service provider to promptly notify the organization of any breach or attempted breach of confidentiality obligations; and
   - The possibility for the organization to request any document and to carry out any verification relating to the confidentiality of the personal information.
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 3 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 4 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.

5.2. Transfers outside of Québec

Transparency. As indicated in section 3.1, BTransparency, 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.

Obligation to conduct a PIA. Transfers of personal information outside Québec are a major concern of the Private Sector Act, as modified by Law 25. 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 the Private Sector Act 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 Private Sector Act does not specify what “generally accepted data protection principles” are and does not define the notion of “adequate protection”. According to the CAI’s PIA Guidance, “adequate protection” refers to protection “that offers legal safeguards (legislation of the destination jurisdiction) and contractual safeguards (agreement with the receiving organization) that comply with generally recognized protection principles and that are appropriate given the sensitivity and the purpose of the personal information involved.” In addition, according to the same guide, generally recognized privacy protection principles are “general rules that ensure the protection of personal information, as well as the respect of the rights and interests of the individuals concerned.”

The CAI also lists several key principles, namely:

- Accountability
- Identifying purposes
- Limiting collection
- Consent
- Privacy by design
- Limiting the use, disclosure, and retention
- Accuracy
- Safeguards

- Transparency
- Individual rights
- Recourses

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.

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.

Best Practices

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 entity 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.
   - position to review these decisions to be responsible for receiving observations from individuals.

→ Continued on next page

Best Practices

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 data protection 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 template (or clauses) 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 5.1, 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.** This 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 5.1 to reflect the requirements for communicating data outside Québec.**

6. Retention and destruction

The Private Sector Act sets out specific requirements for organizations regarding the retention and destruction of personal information.

6.1. Retention and destruction

Retention period. Organizations must retain only the personal information necessary for the purposes for which it was collected. This period corresponds to the time during which the information is held, regardless of its form, medium, or degree of use. During this time, the organization must ensure that the information remains up to date and accurate when it is used to make a decision about an individual, and it must apply security measures appropriate to ensure its protection.

As soon as the personal information is no longer required for the previously determined purposes, it must be securely destroyed or anonymized (see section 6.2 for more details on this alternative). The only exception to this destruction obligation is any statutory retention period (e.g., Canada Business Corporations Act, Income Tax Act, etc.).

Destruction procedure. The destruction method must be adapted to the medium and level of confidentiality of the documents and must ensure the irreversible destruction of the personal information they contain. To ensure the effectiveness of this process, the CAI recommends that organizations implement a records management procedure, designate individuals responsible for its application, and inform all staff.

This procedure must allow the organization to inventory the types of documents containing personal information, define confidentiality levels based on their sensitivity, purpose, quantity, distribution, and medium, and differentiate media so that appropriate retention and destruction methods can be applied. Finally, organizations should implement a retention schedule that complies with legal requirements, noting that the notion of “document” includes all physical or digital media.

Choosing an appropriate destruction method is essential to ensure the permanent destruction of personal information, since a technique suitable for a physical medium (e.g., paper) will not necessarily be suitable for digital media. In this regard, the CAI provides guidance (available in French only) specifying destruction methods appropriate to each type of medium.

The destruction of documents containing personal information may be carried out internally or entrusted to an external service provider when the organization’s equipment does not allow secure destruction. In the latter case, a written contract must govern the service to ensure confidentiality and security, specifying in particular the method used, confidentiality commitments, secure storage, the possibility of an audit by the organization, and the obligation to report any breach. While awaiting transfer to the external provider, the organization remains responsible for properly securing the documents awaiting destruction.

6.2. Anonymization

Definition. Information is considered anonymized when it is "at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly". Anonymized information no longer constitutes personal information and therefore falls outside the legal regime that applies to personal information. Anonymized information is distinct from de-identified information (see section 3.3 for more details).

Possibility of anonymization. The Private Sector Act provides anonymization as an alternative to the destruction of personal information. Therefore, once the purpose for which the information was collected has been fulfilled, it is possible to retain personal information by anonymizing it for serious and legitimate purposes. Note that section 23 does not address anonymization carried out prior to this precise moment in the personal information lifecycle, but only that which occurs after the initial purpose has been fulfilled. That said, this does not mean anonymization is permitted only as an alternative to destruction. In our view, nothing prohibits anonymization at earlier stages of the personal information life cycle.

According to the CAI, anonymizing personal information has important limits: it is practically impossible to guarantee that anonymized information can never be re-identified, especially given technological advances. Certain types of data, such as genetic information, biometric information or geolocation information, are so distinctive that they are particularly vulnerable to potential re-identification. As a result, anonymization remains associated with risks of confidentiality incidents, and any attempt to re-identify a person from such information is subject to sanctions.

Anonymization procedure. Organizations must carry out anonymization of personal information in accordance with "generally accepted best practices" and "according to the criteria and terms set out in the regulation." Under the Regulation respecting the anonymization of personal information, organizations must comply with the following obligations:

- Establish the "serious and legitimate" purposes for which anonymized information will be used.
- Conduct the anonymization process under the supervision of a person who is competent in the field. To do so, organizations should assign supervision to a professional qualified in anonymization and personal information protection or, in the absence of internal expertise, use an external service provider.
- Remove all information that directly identifies the individual concerned (name, contact details, SIN, etc.) before proceeding with anonymization. This data then becomes de-identified information within the meaning of the Private Sector Act.
- Carry out a preliminary analysis of re-identification risks, taking into account factors such as individualization, correlation, and inference, as well as reasonably available information that could be used to identify a person.
- Determine, based on the risk of re-identification, which anonymization techniques to prioritize (e.g., randomization and generalization), ensuring they comply with internationally recognized best practices.

- Establish reasonable protective and security measures to reduce the risk of re-identification, in accordance with the requirements of the Private Sector Act.
- Conduct an analysis demonstrating that the residual risks of re-identification remain very low, taking into account the circumstances, the nature of the information, the criteria of individualization, correlation, and inference, as well as the reasonably available means to re-identify a person. The Regulation on anonymization specifies that this criterion does not require proof of zero risk.
- Perform a periodic assessment of anonymized information, updating the re-identification risk analysis at a frequency determined by previously identified residual risks, to demonstrate that the information remains anonymized. If not, the information ceases to be considered anonymized.
- Maintain an anonymization register that records the description of the anonymized information, the purposes of use, the techniques and security measures applied, and the dates of re-identification risk analysis and their updates. This register must be kept for as long as necessary to allow the organization to demonstrate compliance.

In addition, any organization that collects personal information must establish and implement governance rules addressing, among other things, their destruction, which must include provisions relating to anonymization where applicable.

Best Practices

1. **Develop a clear retention schedule that complies with applicable laws,** specifying for each document category the retention period and when destruction or anonymization must occur.
2. **Implement a records management procedure overseen by designated personnel,** including document inventory, classification by confidentiality level, and staff training.
3. **Select destruction methods that are appropriate for the media and the sensitivity of the information, following CAI guidance and ensuring that data is destroyed permanently and securely.**
4. **Clearly define the serious and legitimate purposes that justify anonymization,** ensuring they are documented and integrated into the organization's governance framework.
5. **Continuously assess and manage re-identification risks** by applying recognized techniques (randomization, generalization) and considering the criteria set out in the Regulation, to ensure residual risks remain very low.
6. **Maintain a complete and up-to-date anonymization register,** including the anonymized information, the purposes of use, the techniques applied, the security measures implemented, and the results of risk analyses, in order to demonstrate compliance at all times

7. Cybersecurity and incident management

The Private Sector Act imposes measures to protect personal information to organizations and makes confidentiality incident reporting mandatory.

7.1. Cybersecurity

Security safeguards. 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. It is important to note that organizations remain responsible for the protection of the information they hold, even when it is in the custody of a third party.

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 PIA.

The CAI provides several examples of measures (available in French only) that organizations should adopt. These include:

- Governance measures (e.g., establishing an information security and privacy committee, and designing and updating governance policies and practices for personal information that are sufficiently robust);
- Tactical measures (e.g., developing an annual action plan and training and raising awareness among employees);
- Operational measures (e.g., granting access rights, developing template models and reviewing them periodically, and using a robust identification protocol);
- Technical measures (e.g., controlling access to offices, server rooms, wiring rooms, alarm systems, and restricting access to premises or filing cabinets where paper documents containing personal information are stored); and
- Technical measures (e.g., promoting strong usernames and passwords, ensuring the encryption of communications and stored information, implementing a firewall, etc.).

The CAI also proposes the following process to ensure the security of personal information:

- Become familiar with and comply with your obligations regarding the protection of personal information;

- Map the personal information held by the organization and assess its sensitivity;
- Identify and analyze risks and their potential effects on the privacy of the individuals concerned;
- Choose security measures that are appropriate to the context and the risks identified above;
- Implement the selected security measures;
- Assess the effectiveness of the measures deployed;
- Ensure ongoing monitoring and review these measures as needed.

Protection measures. The Private Sector Act provides that the Privacy Officer may suggest, at any stage of a project, "measures to protect the personal information" applicable to a project (see section 2.3. on PIAs). 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.

Best Practices

1. **Categorize the information assets to assign security measures that correspond to the level of categorization.**
   - 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 committee that includes the Privacy Officer, and the person responsible for security 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

Confidentiality incident. Québec is 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". The Private Sector Act 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 falls under the application of section 3.6 of the Act. 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.

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 the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") and Alberta's Personal Information Protection Act ("**PIPA**"), as the word "real" has been omitted. In addition, unlike PIPEDA, the Private Sector Act 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:

- **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;
- **The anticipated consequences of its use.** For example, whether the compromised information is likely to be used to commit fraud or identity theft;
- **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 the Private Sector Act test, we do not rule out the possibility that the CAI interprets 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.

Notification of incidents. Ilf 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" under section 3.5 of the Private Sector Act.

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 (see section 5). However, since these notification obligations of the Private Sector Act 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."

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

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:

- 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*;
- The name and contact information of the person to be contacted within that organization with regard to the incident;
- 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;
- A brief description of the circumstances of the incident and what caused it, if known;
- The date or time period when the incident occurred or, if that is not known, the approximate time period;
- The date or time period when the organization became aware of the incident;
- 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;
- A description of the elements that led the organization to conclude that there is a risk of serious injury to the persons concerned;
- The measures the organization has taken or intends to take to notify the persons whose personal information is concerned by the incident, and the date on which such persons were notified, or the expected time limit for the notification;
- 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
- If applicable, an indication that a person or body outside Québec that exercises similar functions to those of the CAI 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 (available in French only) to report a confidentiality incident. This form seems to require more information than what is required under the regulation.

Notices to the persons concerned. The Regulation respecting confidentiality incidents also provides that a notification to individuals affected by a risk of serious harm as a result of a confidentiality incident shall contain::

- 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;
- A brief description of the circumstances of the incident;
- The date or time period when the incident occurred or, if that is not known, the approximate time period;
- 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;
- The measures that the organization suggests the person concerned take in order to reduce the risk of injury or mitigate any such injury; and
- The contact information where the person concerned may obtain more information about the incident.

Mitigation of risk. The Private Sector Act 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.

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 an incident response expert.

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

- 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;
- A brief description of the circumstances of the incident;
- The date or time period when the incident occurred or, if that is not known, the approximate time period;
- The date or time period when the organization became aware of the incident;
- The number of persons concerned by the incident or, if that is not known, the approximate numbers;

- 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;
- 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;
- 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.

For more information on how to prevent confidentiality incidents, please refer to the CAI's explanatory guide and checklist (available in French only).

Special case of entities regulated by the Autorité des marchés financiers (AMF). In October 2024, the Autorité des marchés financiers ("**AMF**") published the Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents ("**AMF Regulation**"). Entered into force in April 2025, the AMF Regulation establishes a rigorous framework to ensure that financial institutions operating in Québec implement proactive measures to manage and report information security incidents. The institutions concerned include insurers, federations and caisses, deposit institutions, trust companies, and credit assessment agents.

The AMF Regulation requires financial institutions to implement a comprehensive information security incident management policy, which must include procedures to detect, assess, and respond to incidents within the organization, as well as those involving third parties to whom activities have been outsourced. This policy must also set out the reporting procedures for incidents to the institution's officers and managers, as well as to any other stakeholders, including potentially consumers, regulatory bodies, and service providers.

When an information security incident that poses a risk of causing negative impacts is reported to an officer or manager of the institution, the institution must in turn inform the AMF within 24 hours. This notice must also cover any incident reported to another law enforcement or regulatory authority, including any confidentiality incident reported simultaneously to the CAI. The notice must be submitted using the form prescribed by the AMF, followed by updates every three days until the incident is under control, and then by a detailed report within 30 days of resolution. The AMF Regulation also requires financial institutions to maintain a register of information security incidents, ensuring the integrity of the data recorded for at least five years. Finally, it provides for the imposition of AMPs in cases of non-compliance.

Best Practices

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 all the 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 all the incident notification obligations to ensure that:**
   - All incidents involving personal information are communicated to the organization promptly;
   - The provisions adequately reflect the 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 organization believes that the incident does not involve serious injury to the individuals involved.

8. Biometrics

8.1. Concepts

Definition of biometrics. 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 Act to establish a legal framework for information technology ("**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. 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.

It should be noted that the CAI adopts a broad and liberal interpretation of the notion of identity verification, considering that the primary objective is to ensure the protection of biometric personal information. To interpret the terms "verification" and "confirmation," the CAI refers to the guidance document of the Office of the Privacy Commissioner of Canada, which distinguishes identification from authentication. It treats identity verification as an identification process aimed at establishing a person's identity by comparing their biometric data with those in a database. It also specifies that identification does not necessarily require a name-based confirmation; it may also result from associating an individual with a small group of previously recorded persons.

Identity. The CAI also adopts an expanded interpretation of the notion of identity, incorporating its digital dimension. It considers that identity is not limited to civil status information, but includes any data that makes it possible to distinguish one person from another. Relying on section 44 of the IT Act, the CAI emphasizes that a person's biometric characteristics are intrinsically linked to their identity. Lastly, the CAI stresses the need for a holistic approach, taking into account the combined effect of all operations rather than examining them in isolation. In other words, it is necessary to consider the combined effect of all operations performed by the system and to treat these different phases as interdependent, since biometric characteristics are inseparable from a person's identity.

8.2 Requirements

The It Act and the Private Sector Act set out certain provisions governing the use of biometric databases to ensure a degree of security. Among the obligations imposed on organizations are the requirement to conduct a PIA, to obtain express consent, and to submit a declaration to the CAI, as described in greater detail below.

Necessity criterion. Organizations must ensure that the collection of biometric information is necessary:

- **The objectives pursued are legitimate, real, and important.** According to the CAI's Biometrics Guide, for an organization to demonstrate the real nature of an objective, it must show that it aims to resolve a specific and actual problem that justifies collecting personal information, especially biometric data. The objective cannot be future-oriented or hypothetical. To determine whether an objective is important, organizations must show that the collection of biometric data is not simply intended to achieve an ordinary, routine, or inherent business objective. According to a CAI decision against Metro inc. (2025) (available in French only), although the desire to control access to premises is a goal that every organization pursues, organizations must provide evidence of a special need to collect and process biometric data in order to better protect their facilities.
- **The impact on individuals' privacy is proportionate to the objectives pursued.** Under the Private Sector Act, the collection of personal information must be proportional to the objectives pursued. Overall, the benefits derived from collecting and processing biometric information must outweigh the impact on individuals' privacy. It is up to organizations to establish that the collection is rationally linked to their objectives, that the privacy impact is minimized, that no less intrusive means exist, and that collecting such information is clearly more beneficial than harmful to the individuals concerned. In the Transcontinental Decision (2025), the CAI concluded that the absence of express consent is sufficient to establish such an impact, regardless of the objective pursued.

It should be noted that the necessity criterion must be strictly met in order to collect biometric data, regardless of whether consent is obtained. That said, the CAI has consistently concluded—save for one exception—that the use of biometrics does not meet the criteria required to reach the threshold of necessity. Most recently, the CAI reiterated that this necessity requirement cannot be bypassed, even when the individual concerned has consented to the collection and use of their biometric data.

PIA. Organizations must carry out a PIA before deploying any biometric system in order to identify legal risks and the controls that must be implemented to mitigate those risks. Note that the PIA may help facilitate the analysis of whether the collection is necessary.

Express consent. Organizations are required to obtain the express consent of individuals for the collection of their biometric data. In addition, because individuals must be free to refuse the collection of their biometric data or withdraw their consent, an alternative solution (e.g., access cards, unique tokens, etc.) must be provided. The CAI has published a model consent form (available in French only) for this purpose.

Declaration to the CAI. Organizations must declare to the CAI the use of any biometric processes or systems intended for the verification or confirmation of identity, as well as the creation of a database of biometric characteristics or measurements. In that case, the declaration must be made at least 60 days before the database is put into service. Without such a declaration to the CAI and express consent, no one may use biometric technologies for the purposes mentioned above. The CAI has published on its website a form for declaring the use of a biometric system. Note that the same form is used for declaring both a biometric system and a database of biometric characteristics or measurements.

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:

Hélène Deschamps Marquis
Partner
T 514.954.3102
hdeschampsmarquis@blg.com

Frédéric Wilson
Partner
T 514.954.2509
fwilson@blg.com

Élisabeth Lesage-Bigras
Senior Associate
T 514.395.2749
elesagebigras@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

Matt Saunders
Counsel
T 514.954.3185
msaunders@blg.com

Cléa Jullien
Associate
T 514.954.3121
cjullien@blg.com

© 2026 Borden Ladner Gervais LLP. BD12907–02–26