Consumer Privacy Protection Act (Canada's Bill C-27): Feedback from industry participants

January 30, 2023

Bill C-27 – the second iteration of Bill C-11 (2020), which died on the order paper in 2021 – is currently at second reading in the House of Commons. Canada's *Consumer Privacy Protection Act* introduces two new statutes that would make substantial changes to the federal data protection legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). First, the *Consumer Privacy Protection Act* (CPPA) would replace Part 1 of PIPEDA, which relates to the protection of personal information. Second, the *Personal Information and Data Protection Tribunal Act* (PIDPT) would create a new Data Protection Tribunal.

Bill C-27 also introduces the *Artificial Intelligence and Data Act* (AIDA), which would create a new legal and general framework for the regulation of artificial intelligence (AI). During the second reading of Bill C-27, it was suggested that AIDA be voted on separately from the privacy aspects of the Bill, namely CPPA and PIDPT. The proposal aims to operationalize the Canadian government's Digital Charter as well as past proposals to strengthen privacy in the digital age in order to address the challenges posed by the digital economy and new technologies.

The most serious violations of the CPPA could result, upon prosecution, in fines that have been described as the strongest among G7 privacy laws, including the European Union's General Data Protection Regulation (GDPR) and the *California Consumer Privacy Act of 2018* (CCPA). While clearly inspired by similar initiatives in other countries, namely the GDPR and the CCPA, the Canadian proposal is unique in its approach in that, in many instances, it affords businesses greater flexibility and clarity relative to the present privacy regime's requirements. Most notably, it borrows directly from past guidance and decisions issued by the federal privacy commissioner, the Office of the Privacy Commissioner of Canada (Commissioner), and provides individuals with new rights that are more narrowly framed than those currently found under the GDPR.

It should also be noted that Québec's private-sector data protection regime, the Québec *Act respecting the protection of personal information in the private sector* (Québec *Private Sector Act*), as modified by Bill 64 (Bill 64), is in many respects more onerous than the CPPA, raising a number of challenges from an interoperability standpoint for businesses operating at a national level. For a summary of the key differences between the rights and obligations under C-27 and Bill 64, see Schedule "A" at the end of this

article. For a detailed analysis of the changes introduced by Bill 64, please review our Bill 64 Compliance Guide.

Parliament has invited input from industry participants regarding Bill C-27. Various organizations and industry stakeholders have recently raised legal and operational concerns with some of the proposed provisions of this bill, especially regarding those that could have unintended or inimical effects. In that context, this article provides an overview of some of these concerns, with a focus on the CPPA, and summarizes certain salient points that industry participants may consider raising in their commentary on Bill C-27. This article does not cover all submissions presented by various industry-specific organizations nor does it provide a complete overview of all such concerns.

Enforcement

The CPPA introduces major changes to PIPEDA, including to the current enforcement regime with the introduction of order-making powers. It also introduces a new tribunal empowered to issue large penalties and a broad private right of action.

i. Reducing maximum penalties

The CPPA will grant new order-making powers to the Commissioner**.** Further, the Commissioner will have the power to make recommendations to the Data Protection Tribunal (the Tribunal) for the imposition of penalties of up to the greater of C$10,000,000 or **three per cent** of the organization's global gross revenue for violations of certain provisions set out in section 94 of the CPPA. These maximum penalties would be among the highest in the world. We note, for example, that administrative fines under the GDPR (Art. 83(4)) and the administrative monetary penalties under Québec Bill 64 are in some cases capped at **two per cent** for similar violations.

Further, the most egregious CPPA violations would constitute offences punishable, upon prosecution, by a fine of up to the greater of C$25,000,000 or **five per cent** of the organization's global gross revenue. This cap is higher than that currently found in either the GDPR (Art. 83(5)) or Québec Bill 64, which is at four per cent for certain violations (although Québec Bill 64 provides for the doubling of fines for subsequent offences).

In general, the maximum penalties and fines under the CPPA should be harmonized with the caps set out in the amended Québec *Private Sector Act*, namely 2 per cent for administrative monetary penalties and 4 per cent for fines, and should not exceed, depending on the nature of the violation, similar caps on administrative fines under the GDPR.

ii. Reasonable transition period

Although the CPPA introduces significant changes to PIPEDA, the transition period for organizations to prepare for these changes is not clearly set out in Bill C-27. Before developing and implementing a privacy compliance plan, an organization must typically analyze its current practices and conduct a gap assessment, which may include steps such as conducting data mapping exercises, creating data inventories and reviewing and updating vendor agreements. This may also include revising privacy policies and programs, and developing procedures and systems to address new individual rights

such as data portability, disposal, and explanation (of certain predictions, recommendations, or decisions resulting from an automated decision system). Depending on the size of the organization and the maturity level of its privacy programs, an organization may need at least 24 to 36 months to prepare for these changes.

Other privacy laws such as Québec Bill 64 and the GDPR have generally provided organizations with a transition period of at least two years. Given the time required for organizations to fully prepare for these changes and the precedent set by other privacy laws, it is recommended that the CPPA include a reasonable transition period that reflects these considerations. This will give organizations sufficient time to prepare, as well as allow for the Commissioner to issue directives and guidance, and for the government to publish related regulations.

Retention of personal information

The CPPA introduces new requirements relating to the retention of personal information, which could present practical challenges for organizations (see also the Right of disposal section of this article).

i. Limited transparency requirements for retention periods

Section 62(2)(e) of the CPPA requires an organization to make readily available information about its privacy management policies and practices, including the "retention periods applicable to sensitive personal information." However, an organization may be reluctant to publish and share this type of information, as this could draw the attention of cyber criminals to high-value data repositories. In addition, it may not always be possible for an organization to provide the specific periods of time for which sensitive personal information will be retained, as this period may depend on a number of criteria, such as the occurrence of a future and uncertain event.

More generally, it may be difficult for an organization to identify all categories of personal information that may be considered "sensitive," as this term is not clearly defined under the CPPA and requires consideration of various contextual factors. For example, while certain categories of personal information will almost always be considered sensitive (such as health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious or philosophical beliefs) or will be deemed sensitive (for instance, personal information of minors), other categories of personal information may only be sensitive in certain situations. It is therefore reasonable to expect that compliance with this requirement will vary considerably from one organization to another, as it may not be readily apparent in all cases whether the information held by an organization is sensitive within the meaning of the CPPA.

For these reasons, it may be more appropriate to require an organization to provide a "general account" of its retention practices as a whole, regardless of the sensitivity of the information. This would be consistent with section 62(2)(b) and (c), both of which require an organization to make available a "general account" of the organization's use of personal information. This suggestion would also better align with existing decisions under PIPEDA in which the Commissioner has held that individuals should be able to

obtain information about an organization's general retention policy without unreasonable effort.

Consent

The CPPA makes significant changes to the rules governing consent to the collection, use and disclosure of personal information. The CPPA introduces a consent exception regarding specified "business activities" and a more flexible consent exception for certain processing operations carried out for the purpose of an activity in which the organization has a "legitimate interest." The CPPA also deems minors' personal information to be sensitive regardless of the actual nature of the information or the context in which it is processed and as a result, may require express consent whenever an organization is dealing with the personal information of a minor unless a consent exception applies.

Businesses welcome that the CPPA seeks to strike a better balance between the legitimate business interests of organizations in processing personal information and the privacy rights of Canadians. However, certain aspects of these new provisions pose potential operational challenges for organizations.

i. New consent exceptions applying to the disclosure of personal information

The CPPA introduces new consent exceptions designed to facilitate the collection and use of personal information for the purposes of a "business activity" listed in subsection 18(2) and an "activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual," as defined in subsection 18(3). While similar language is found in the GDPR, which creates a separate legitimate interest basis for processing personal data (see Art. 6(1)(f); recital 47), it is important to note that the CPPA differs in two key areas.

First, the CPPA's business activities and legitimate interest exceptions are just that: exceptions to the consent requirement. As such, they are not separate legal bases for processing personal information on the same footing as consent. This is important because courts tend to interpret consent exceptions narrowly, which is likely to favour a narrower interpretation of these new exceptions.

Second, these exceptions are limited to the collection and use of personal information, meaning that a disclosure to a third party for the purpose of a "business activity" or an "activity in which the organization has a legitimate interest" would not be permitted, notwithstanding that appropriate measures have been taken to mitigate the risk of harm resulting from the disclosure. For example, an organization may need to share personal information with a number of third parties to "provide a product or service" requested by an individual (s. 18(2)(a)). This may include payment processors, package delivery providers, financial institutions and other third-party intermediaries that merely facilitate a commercial transaction. While some of these third parties may be considered service providers (and benefit from a separate consent exception), others may play a role closer to that of an independent controller.

Similarly, the exception for activities in which an organization has a legitimate interest may in some cases create an arbitrary distinction between the collection and use of personal information and its disclosure. For example, an organization may collect and use personal information to measure and improve the use of its services. This may arguably fall under the legitimate interest exception, provided that the organization has a clear interest in improving its services that outweighs any potential adverse effects on individuals and takes appropriate steps to assess and mitigate those effects (s. 18(4)). However, if the same organization were to disclose the personal information for the same purpose to a third-party vendor that provides the same services on behalf of the organization (and possibly other business customers), that disclosure may not be covered by the exception.

For these reasons, the exceptions to consent for business and legitimate interest activities could be revised to permit certain types of disclosure to a third party. Of course, this disclosure should be subject to appropriate accountability mechanisms, such as contractual measures limiting the third party's use of the information and a prior assessment of the impact of the disclosure on the interests of the individual.

ii. Overlap between implied consent and new consent exceptions

As discussed above, the CPPA allows organizations to **collect and use** personal information without the individual's knowledge and consent for a "business activity" (as this term is defined, see subsections 18(1) and (2)) or when the organization has a "legitimate interest" that outweighs any potential adverse effect on the individual. However, to rely on this exception, the organization must prepare and document a legitimate interest assessment (subsection 18(3)).

Section 15(6) of the CPPA further prevents organizations from relying on implied consent to collect and use personal information in these situations (that is, when the collection and use of information are governed by the "business activity" or "legitimate interest" consent exceptions). This prohibition may create operational challenges for organizations, since there may often be an overlap between situations whereby organizations can currently collect and use personal information relying on the individual's implied consent, and situations in which they may also have a legitimate interest.

In these overlapping situations, an organization should be entitled to rely on implied consent, which may involve providing an additional notice to individuals, without having to conduct a legitimate interest assessment.

iii. Exclusion of marketing activities from the "legitimate interest" exception

Subsection 18(3) of the CPPA excludes from the "legitimate interest" exception any situation where personal information is collected or used for the purpose of influencing the individual's behaviour or decisions. While it is not readily clear what activities would be considered to be undertaken for the purpose of influencing an individual's behaviour or decisions, a strict application of this criterion could lead to the exclusion of a wide range of marketing activities, regardless of the sensitivity of the information or the reasonable expectations of individuals.

It should be noted that even the GDPR regards direct marketing as a "legitimate interest" in some situations. Subsection 18(3) could be revised to specify that the words "influencing the individual's behaviour and decisions" refer either to specific types of practices (such as behavioural advertising activities or decisions that could have a significant impact on individuals) or to practices that may go against the reasonable expectations of individuals.

iv. Limited scope of the "socially beneficial purposes" consent exception

Section 39 of the CPPA creates a new consent exception for disclosures of de-identified personal information to specific public sector entities, including government, healthcare and post-secondary educational institutions, as well as public libraries in Canada.

Limiting this consent exception only to disclosures to public sector entities instead of public and private sector entities severely restricts its utility. This section 39 could be reviewed to authorize and facilitate responsible data sharing between a broader range of actors (including private sector organizations) which may have access to talent and resources that they can leverage to pursue socially beneficial purposes. This review should include the introduction of additional oversight requirements and data protection practices, such as the implementation of specific contractual measures and a requirement to conduct a privacy impact assessment before relying on this consent exception.

v. Minors' personal information and sensitivity of personal information

Section 2(2) of the CPPA considers minors' personal information as sensitive information and section 15(5) requires organizations to consider the sensitivity of information when determining the appropriate form of consent. These two provisions could be read as requiring that organizations obtain express consent whenever they are processing personal information of minors, which may be unrealistic in certain situations and may trigger operational challenges. For instance, an organization may not have knowledge or have any way of knowing whether it is in fact processing minors' personal information. It could also be required to collect additional sensitive personal information to determine if it is dealing with minors.

A more practical approach would be to consider personal information of minors as sensitive personal information only when organizations have actual knowledge, or ought to know, that they are dealing with minors. In these cases, they would be required to treat this personal information as sensitive information.

Right of disposal

Similarly to PIPEDA, the CPPA grants individuals the right to access and amend their personal information held by organizations. The CPPA also introduces new individual rights, such as a data disposal right in section 55, which raises certain concerns.

i. Right of disposal exception and minors' information

Subsection 55(2) of the CPPA provides for exceptions to the right of disposal. However, some of these exceptions do not apply to personal information of minors. For example,

an organization may have to comply with a request to dispose of a minor's personal information, even if the disposal would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual.

This exclusion should only apply in limited circumstances, such as when retaining the information may create residual risk to minors (for example, risk to the minors' reputation in cases where the information is published).

ii. Right of disposal and additional exceptions for fraud management and investigations

The right of disposal introduced in section 55 of the CPPA should also introduce an exception for any personal information that the organization can collect without the individual's knowledge or consent, such as personal information collected for fraud management or investigation purposes. This would allow organizations to refuse to dispose of personal information if this information is necessary for a legitimate business need, such as fraud management or conducting an investigation.

De-identification, research and analytics

The CPPA introduces new definitions for the terms "anonymize" and "de-identify" and provides greater flexibility regarding the processing of these categories of information, including for internal research and analytics purposes. However, these definitions might create practical challenges for organizations. Please note that the Canadian Anonymization Network has published an in-depth analysis of these challenges in their publication, *Proposed amendments to the de-identification and Anonymization provisions in the Digital Charger Implementation Act, 2022 (Bill C-27)*, which should be read alongside this section.

i. Absolute standard for anonymization may not be appropriate

For data to be considered "anonymized" under the section 2(1) of the CPPA, it must be "irreversibly and permanently modif[ied]…, in accordance with generally accepted practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means." The proposed standard is more stringent than other recently updated privacy legislation. For example, under the amended Québec *Private Sector Act*, personal information is anonymized "if it is at all times **reasonable to expect** in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly." The CPPA should include a similar reasonableness standard, instead of holding organizations accountable to an absolute standard that may be impossible to meet in practice.

ii. Rules regarding re-identification should be more permissive

While it is important to preserve the layer of privacy protection that de-identification provides to individuals, the list of situations stated in section 75 of the CPPA in which organizations may re-identify individuals may be too limited. There are several innocuous cases in which an organization may need to re-identify data that it had

previously de-identified. For example, in certain cases, re-identification may be relevant to suppress or investigate fraud This section may therefore be reviewed to authorize re-identification with the individual's consent or in situations where the processing of personal information is permitted without consent.

iii. Use of de-identified information for research, analysis and development purposes

Section 21 of the CPPA introduces a new consent exception for the use of de-identified information for "internal research, analysis and development purposes." This would enable organizations to use personal information for a range of innovative purposes, provided they de-identify the information beforehand. Restricting the use of de-identified data to **internal** uses by the organization may limit the collaboration and the fostering of research partnerships. These partnerships are crucial, as they allow stakeholders to share datasets to create data pools that are broad enough for the production of useful and actionable insights.

This section could be reviewed to authorize the use and sharing of de-identified information amongst different organizations subject to industry best practices regarding confidentiality, data security, and additional restrictions to adequately protect individuals (which may include specific contractual measures and a requirement to conduct a privacy impact assessment).

Automated decision systems and AI

Under subsection 62(2)(c) of the CPPA, an organization using an automated decision system will need to make readily available, in plain language, a general account of the organization's use of such a system to make predictions, recommendations or decisions about individuals that could have a significant impact on them.

i. Broad definition of automated decision systems

Section 2(1) of the CPPA defines automated decision systems as "any technology that **assists or replaces** the judgment of human decision-makers." Contrary to the GDPR and the Québec *Private Sector Act*, both of which define an automated decision system as one that is fully automated, the CPPA's scope is considerably broader given that it includes a system that simply **assists** in the judgment of human decision-makers. This may trigger a situation where organizations will have to provide information and respond to individuals' requests regarding a potentially large number of decisions which humans make daily with the assistance of widely available technology (that is, e-discovery, accounting software, etc.), provided such decisions have a significant impact on individuals concerned. The CPPA's definition of automated decision systems should be reviewed and harmonized with other privacy statutes by limiting its scope to fully automated systems.

ii. Refusal for requests made in bad faith

Section 63(3) of the CPPA allows an individual to request an explanation for any automated decision, prediction or recommendation that could have a significant impact

on them. Section 55(2)(e) of the CPPA allows organizations to refuse disposal requests that are either vexatious or that have been made in bad faith, but this right of refusal is not included for other types of requests, including those for explanations regarding automated decision-making processes. It should be noted that the GDPR allows organizations to refuse all types of user requests that are either manifestly unfounded or excessive, for instance because of their repetitive nature (see art. 12 of the GDPR). Given the number and volume of access requests that organizations have had to manage over recent years (some of which were repetitive or made in bad faith), and the fact that these organizations may also be subject to a large volume of requests for explanations regarding their automated decision systems, a similar exception could also be considered for these types of requests.

Next steps

As Bill C-27 remains at second reading in the House of Commons, we can expect further developments in the coming months as C-27 moves through the legislative process. Industry participants may communicate their submissions to the government, and industry leaders will be invited to discuss and testify about the proposed bill.

The BLG Privacy and Data Protection team will be providing additional insights on this new bill over the next few months. We will hold webinars and prepare checklists and publications focusing on specific issues.

We invite you to communicate with one of the key contacts below to discuss the points raised in this article further, and to consult our in-depth article for a full summary of changes contemplated by Bill C-27.

Schedule "A"

Table comparing key differences between Bill 64 (Québec) and C-27 (federal)

	Bill 64 (Québec)	**Bill C-27 (federal)**
Automated decision-making	An organization will be required to inform individuals that their personal information has been used to make a *decision based exclusively on an automated processing of the information*, no later than the time it informs the individual of the decision. In addition, individuals are granted the right to be informed, upon request, of the personal	An organization will be required to include in its public-facing privacy policy "a general account of [its] use of any automated decision system to make *predictions, recommendations or decisions* about individuals that could have a *significant impact on them*" (s. 62(2)(c), CPPA). In addition, individuals are granted the

	Bill 64 (Québec)	Bill C-27 (federal)
	information that was used to make the decision, as well as the reasons and the principal factors and parameters that led to that decision. Individuals are also given the right to submit observations to an employee who is in a position to review the decision (s. 12.1, Québec *Private Sector Act*).	right to be provided an explanation of the prediction, recommendation or decision. This includes information about the personal information that was used to make the decision, the source of the information, as well as the reasons and the principal factors that led to that prediction, recommendation or decision. Note that an "automated decision system" is defined as "any technology that *assists or replaces* the judgment of human decision-makers" through various techniques such as machine learning and neural networks (s. 2(1), CPPA). As such, this definition is not necessarily limited to decisions based solely on automated processing.[1]
Privacy impact assessment (PIA)	An organization will need to conduct a PIA in a wide range of situations, particularly where a project involves the acquisition, development or overhaul of an "information system" or "electronic service delivery system" involving the processing of personal information. Note that the PIA should be proportionate to the risk posed by the project, taking into account, among other things, the sensitivity of the information involved and the purposes of the processing. (s. 3.3)	No mandatory PIA, although this is usually a practice recommended by the Commissioner, especially when processing activities are considered privacy intrusive. Note, however, that organizations wishing to collect or use personal information without consent for an activity carried out in their legitimate interests will need to conduct a "legitimate interest assessment" or "LIA" (s. 18(3)(4)(5), CPPA). The LIA will need to assess, among other things, the risks resulting from the activity

	Bill 64 (Québec)	Bill C-27 (federal)
		and the measures in place to reduce those risks.
Cross-border transfer, and transfer impact assessment (TIA)	If personal information is "communicated" outside Québec, whether to a service provider or another category of third party, the organization will be required to conduct a privacy impact assessment related to the transfer (also referred to as a "transfer impact assessment" or "TIA") and enter into a contract with the third party. The TIA must take into account various prescribed factors, such as the applicable legal framework in the state where the information would be disclosed, and is intended to determine whether the information would receive "adequate protection, in particular in light of generally recognized principles regarding the protection of personal information." Information may only be transferred outside of Québec if the assessment confirms that the information would be adequately protected and that a written agreement between the parties has been entered into containing appropriate data protection clauses (s. 17, Québec *Private Sector Act*). In addition, the party collecting the information must inform individuals at the time of collection that their	No mandatory TIA, but must indicate in a public-facing privacy policy "whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications" (s. 62(2)(d), CPPA).

	Bill 64 (Québec)	Bill C-27 (federal)
	personal information may be communicated outside Québec (s. 8, Québec *Private Sector Act*).	
Right to data portability / mobility	Individuals will have the right to obtain a copy of the personal information they have provided to an organization in a "structured, commonly used, and technological format," and to have the information transferred to any person or body authorized by law to collect such information, subject to certain exceptions.[2] This right applies only to computerized personal information that is collected from the individual, which means that it excludes information that has been created or inferred using personal information (s. 27, Québec *Private Sector Act*).	Individuals will have a right to data mobility. The right to data mobility is more limited than the right to data portability in Québec. Indeed, it only grants individuals the right to have the personal information they have provided to an organization transferred to another organization if both organizations are subject to a "data mobility framework" (s. 72, CPPA). In other words, it does not include the right to request a copy of the information in a particular format. In addition, the rules, parameters, safeguards and exceptions surrounding these data mobility frameworks will be determined by future regulations (s. 123, CPPA).
Right to be forgotten	Individuals will have the right to request the de-indexation of hyperlinks associated with their name or to request that an organization cease disseminating their personal information in certain situations, such as when the dissemination of the information contravenes the law or a court order, or causes serious injury to the	There is no specific right to request the removal of hyperlinks or to cease the dissemination of personal information, but there is a right to request disposal of personal information in certain situations (see below).

	Bill 64 (Québec)	Bill C-27 (federal)
	individual's reputation or privacy. In the latter case, the organization will need to assess certain conditions and factors to determine whether to grant or deny the request (s. 28.1, Québec *Private Sector Act*).	
Right to disposal	No specific right to disposal of information, but an individual may be permitted to request deletion in situations that give rise to a right of rectification, particularly where the information was collected, disclosed or retained unlawfully (s. 28, Québec *Private Sector Act*).	Individuals will have the right to request disposal of personal information under the organization's control in certain situations, such as where the information has been collected, used or disclosed unlawfully, the individual has withdrawn consent, or the information is no longer required for the provision of a product or service requested by the individual. Note that there are various exceptions to this right (such as where retention is necessary to comply with legal or contractual obligations) (s. 55, CPPA).
Anonymization	Information that has been adequately anonymized is no longer considered "personal information" under Québec *Private Sector Act*. However, information is only considered anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the individual to be identified	Information that has been adequately anonymized is no longer considered "personal information" under the CPPA. However, information is only considered anonymized if it is irreversibly and permanently modified, in accordance with generally accepted best practices, to ensure that no individual can

	Bill 64 (Québec)	Bill C-27 (federal)
	directly or indirectly. An organization must also ensure that the information is anonymized according to generally accepted best practices, and in accordance with the criteria and procedures prescribed by future regulations. In addition, information that is no longer required to fulfill the purposes for which it was collected and used can be anonymized but only for "serious and legitimate purposes" (s. 23, Québec *Private Sector Act*).	be identified from the information, whether directly or indirectly, by any means (s. 2(1), CPPA). Note that in some respects, this standard of anonymization may be slightly higher than that imposed by the Québec *Private Sector Act*.
New consent exceptions	New consent exceptions will be available for the following processing activities: • The use of personal information for purposes (other than philanthropic or commercial prospection) that are consistent with those for which it was originally collected (s. 12 para. 2(1), Québec *Private Sector Act*); • The use of personal information for the provision of a product or service requested (s. 12 para. 2(4), Québec *Private Sector Act*); • The use of personal information to prevent or detect	New consent exceptions will be available for the following processing activities: • The collection and use of personal information for legitimate business activities, such as the provision of a product or service requested or safety-related purposes, subject to certain conditions (s. 18(1)(2), CPPA); • The collection and use of personal information for activities carried out in the organization's legitimate interests, subject to certain conditions (s. 18(3)(4)(5), CPPA);

	Bill 64 (Québec)	Bill C-27 (federal)
	fraud or to assess and improve protection and security measures (s. 12 para. 2(3), Québec *Private Sector Act*); • The use of de-identified information for study, research or statistical purposes (s. 12 para. 2(5), Québec *Private Sector Act*); • The disclosure of personal information to any person or body wishing to use the information for their own study, research or statistical purposes, subject to the conduct of a PIA that takes into account prescribed elements and entering into an agreement with a third party that contains relevant data protection clauses (ss. 21-21.0.2, Québec *Private Sector Act*).	• The use of de-identified information for internal research, analysis and development purposes (s. 21, CPPA); • The disclosure of de-identified information to government institutions or other prescribed category of third party, for a socially beneficial purpose (related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose) (s. 39, CPPA).
Profiling and location tracking	Organizations that collect personal information using technology that includes functions that profile, locate or identify the individual must inform the individual, at the	No specific requirements on technologies that profile, locate or identify individuals. Instead, these functions are subject to general notice and consent rules, meaning that

	Bill 64 (Québec)	Bill C-27 (federal)
	time of collection, of the use of this technology and the means to activate these functions on their own. Organizations must also ensure that these functions are deactivated by default, which means that users must take an affirmative action to signify their agreement to activate certain functions such as profiling and locating (s. 8.1, Québec *Private Sector Act*).	consent may be express or implied depending on the sensitivity of the information collected and the reasonable expectations of individuals. Note that precise location data (for example, see OPC, *PIPEDA Findings #2022-001*, June 1, 2022) and highly detailed and rich multidimensional profiles are generally considered sensitive (for example, see OPC, *PIPEDA Report of Findings #2015-001*, April 7, 2015, para. 73) which means that express consent (opt-in) is typically required for this collection.
Default privacy settings	Organizations that collect personal information through technological products or services offered to the public (other than browser cookies) must ensure that all privacy settings are set to provide "the highest level of confidentiality by default" (s. 9.1, Québec *Private Sector Act*). It is not entirely clear what will be considered the highest level of confidentiality by default in a given situation, as this term is not defined in the legislation.	No specific requirements on default privacy setting. Note that the Commissioner has taken the position that these settings should be set in accordance with the reasonable expectations of individuals. For example, see OPC, *PIPEDA Report of Findings #2018-004*, June 20, 2018, at para. 56: "Our Office has previously held that when an organization preselects default settings, such settings must accord with users' reasonable expectations and users must be properly informed of the settings and of the implications of choosing one setting over another."

[1] This is one of the key distinctions between the automated decision-making provisions of the CPPA and those of the Québec *Act Respecting the Protection of Personal*

Information in the Private Sector (ARPPIPS). Note that the Québec ARPPIPS also provides a separate right to submit observations to an employee who is in a position to review the decision, whereas the CPPA does not provide an equivalent right.

[2] For example, an organization may refuse to grant a request for data portability if doing so "raises serious practical difficulties" or "would likely reveal personal information about a third person or the existence of such information and the disclosure may seriously harm that third person." See sections 27, 39 and 40, ARPPIPS.

By

Simon Du Perron, Daniel-Nicolas El Khoury, Marc Vani, Andy Nagy

Expertise

Cybersecurity, Privacy & Data Protection
