BLG
Borden Ladner Gervais

Canada's *Consumer Privacy Protection Act* (Bill C-27):

Impact for businesses

June 2022

On June 15, 2022, the Minister of Innovation, Science and Industry, François-Phillippe Champagne introduced Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* (or *Digital Charter Implementation Act, 2022*). This long-awaited piece of legislation is in a sense the faithful successor of the former Bill C-11, tabled in 2020, which died on the order paper in August 2021 ("**C-11 (2020)**").

Bill C-27 reintroduces two Acts that will sound familiar for those who followed Bill C-11 (2020), namely the *Consumer Privacy Protection Act* ("**CPPA**") and the *Personal Information and Data Protection Tribunal Act*. The novelty of C-27 primarily lies in the introduction of a third legislation, the *Artificial Intelligence and Data Act* ("**AIDA**").

Bill C-27 seeks to replace the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") with a modernized and stronger privacy and data protection legal framework in Canada. This article focuses on the key differences between the proposed legislation and the actual federal privacy regime in the private sector governed by PIPEDA.

Table of Contents

What you need to know

This article provides an overview of the key aspects of the CPPA and their impact on Canadian businesses.

As more fully detailed herein, the CPPA is introducing a new privacy regime that would introduce the following changes, which were already introduced with C-11 (2020) and have not changed with this new version of C-27:

- New enforcement tools:
    - The newly constituted Personal Information and Data Protection Tribunal would have powers to impose, upon recommendation by the Office of the Privacy Commissioner of Canada, administrative monetary penalties of C$10,000,000 or, if greater, the amount corresponding to three per cent of the organization's global gross revenues in its previous fiscal year.
    - Reinforced fines in the case of penal proceedings for a maximum of C$25,000,000, or, if greater, the amount corresponding to five per cent of the organization's global gross revenues in its previous fiscal year.
    - New private right of action for individuals.
    - New provisions to enable the creation of "codes of practice" and "certification programs".
- New individual rights inspired by European law: right to be informed of automated decision-making, right to disposal and right to mobility.
- Reinforced accountability rules:
    - New definition of the notion of "control".
    - New obligation to establish, implement and make available a privacy management program.
    - Clarity concerning the role and responsibilities of service providers.
- Reinforced consent requirements, including greater clarity concerning the notion of valid consent.
- Some less stringent rules: new consent exceptions for de-identified information and legitimate business practices.

The new version of the CPPA (C-27) is also introducing new changes from the previous version C-11 (2020). To assist you in your review of Bill C-27, we have prepared a comparative chart describing the most significant changes introduced by C-27 compared to C-11 (2020). More specifically, we have summarized these key changes at the beginning of each section.

Introduction

The federal government's proposal to modernize the *Personal Information Protection and Electronic Documents Act* (PIPEDA) – a legislation that was enacted nearly two decades ago, is as ambitious as it is cautious in its attempt to meaningfully enhance privacy protections for individuals. The proposal, which would effectively replace PIPEDA's privacy provisions with the *Consumer Privacy Protection Act* (CPPA), 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 novelty of C-27 primarily lies in the introduction of a third legislation, the Artificial Intelligence and Data Act ("AIDA"). Otherwise, the proposal is relatively similar to C-11 (2020) as it would enact the *Personal Information Data Protection Tribunal Act*, establishing a new Personal Information and Data Protection Tribunal, which would have the ability to impose significant penalties. Further, the most serious violations of the CPPA could result, upon prosecution, in fines, which 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 EU's GDPR and California's CCPA, the Canadian proposal is unique in its approach in that, in many instances, it affords businesses with 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. In this sense, it bears noting that on many aspects, 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 considerably more onerous than the CPPA, raising a number of challenges from an interoperability standpoint for businesses operating at a national level. For a more detailed analysis of Québec Bill 64's proposed amendments, please see review our Compliance Guide on Bill 64.

The differences between Québec Bill 64 and the CPPA highlight the importance of enhancing consistency among different privacy law regimes, especially as Canada's adequacy status under the GDPR, which affords Canadian businesses handling personal data that is subject to the GDPR with a competitive advantage, is currently up for review. Furthermore, we can expect similar talks of reform concerning the Alberta *Personal Information Protection Act* (Alberta PIPA) and the British Columbia *Personal Information Protection Act* (BC PIPA), which, in addition to the Québec Private Sector Act, are deemed "substantially similar" to PIPEDA and therefore apply in lieu thereof for intra-provincial privacy matters. Indeed, in December 2021, a special committee appointed by the British Columbia Legislative Assembly published a report recommending significant changes to the BC PIPA. In addition, in June 2021, the Ontario Government published a white paper that sets out a model for a first private-sector privacy law statute for this province (see "*Ontario moves forward with privacy legislation initiative*").

Enforcement

Enforcement - Summary of changes in C-27 from the previous version C-11 (2020)

- Procedural changes regarding the Commissioner's investigations (ss. 83, 84, 85).
- **Key change** → Contraventions to additional provisions are subject to a penalty, namely: (i) privacy management program (s. 9), (ii) transfers to service providers (s. 11), (iii) purpose limitation (s. 12(3) and (4)), (iv) requirement to obtain consent (s. 15(1)), (v) prohibition to force consent when not a condition of service (s. 15(7), (vi) consent obtained by deception (s. 16), (vii) withdrawal of consent (s. 17(2)), (viii) retention (s. 53), (ix) service provider obligation to report breach to the organization (s. 61), (x) making available information about policies and practices. (s. 62(1)). (s. 94(1))
- **Key change** → The Commissioner must take into account new factors in deciding whether to recommend that a penalty be imposed by the Tribunal: (i) evidence that the organization exercised due diligence to avoid the contravention; (ii) whether the organization made reasonable efforts to mitigate or reverse the contravention's effects; (iii) any prescribed factor. (s. 94(2))
- The Commissioner's power to audit an organization's personal information management practices extends to situation where the Commissioner has reasonable grounds to believe that the organization is contravening or likely to contravene the CPPA. (s. 97)

The CPPA introduces major changes to the federal privacy enforcement regime which will create significant compliance risks for businesses. Most notably, the CPPA will grant new order-making powers to the Commissioner. Additionally, the Commissioner may make recommendations to the Tribunal for the imposition of penalties of up to C$10,000,000 or three per cent of the organization's global gross revenues, whichever is higher. In contrast, equivalent fines under the GDPR and Québec Bill 64 use a cap of two per cent. Further, the most egregious CPPA violations would constitute offences punishable, upon prosecution, with a fine up to C$25,000,000 or five per cent of the organization's global gross revenues. This upper limit is higher than the one currently found in either the GDPR or Québec Bill 64, which is capped at four per cent (although Québec Bill 64 provides for the doubling of fines for subsequent offences).

Powers of the Commissioner

Current powers maintained – investigations, compliance agreements and audits. The CPPA carries forward certain powers found in PIPEDA including that individuals may file complaints or the Commissioner can initiate a complaint on its own initiative (s. 82 CPPA replacing s. 11 PIPEDA). The Commissioner also maintains the following powers:

- Carrying out investigations in respect of a complaint (s. 83 CPPA replacing s. 12 PIPEDA);
- Entering into compliance agreements with organizations who have contravened the statute (s. 87 CPPA replacing s. 17.1 PIPEDA); and
- Conducting audits regarding an organization's compliance with the statute (s. 97 CPPA replacing s. 18 PIPEDA).

New powers – compliance orders and recommendations of penalties. The CPPA, however, will grant the Commissioner new powers to conduct an inquiry after investigating a complaint (s. 89) or non-compliance with a compliance agreement (s. 90). At the conclusion of an inquiry, the Commissioner is required to render a decision in which it may issue a compliance order (s. 93), if the Commissioner finds that organization has contravened the CPPA.

- **Compliance orders.** The CPPA would grant the Commissioner significant new powers to order organizations to do the following:
    - Take measures to comply with the statute;
    - Stop doing something that is in contravention of the statute;
    - Comply with a compliance agreement; and
    - Make public any measures to correct its policies, practices or procedures (s. 92(2)).

    An organization will be able to appeal a compliance order to the Tribunal, as discussed below. However, if the compliance order is not appealed, it will be enforceable in the same manner as an order of the Federal Court (s. 104).
- **Penalty recommendation.** The Commissioner is also required to decide whether to make a recommendation that the Tribunal impose a penalty for violating the CPPA's key provisions (s. 94). Unlike privacy regulators under other regimes (*e.g.*, the GDPR and Québec Bill 64), the Commissioner will not have powers to directly impose penalties for CPPA violations.

Monetary penalties imposed by the Tribunal

The Tribunal will have the power to impose a penalty on an organization after giving the organization and the Commissioner the opportunity to make representations and if the Tribunal determines that it is appropriate to do so (s. 95(1)). The Tribunal must rely on either the Commissioner's findings or its own findings in the case of appeal (s. 95(2)). Significantly, organizations will have a defence of due diligence (s. 95(3)).

The maximum penalty for all the contraventions in a recommendation taken together is the higher of C$10,000,000 and three per cent of the organization's gross global revenue in its financial year before the one in which the penalty is imposed (s. 95(4)). The statute sets out the factors that the Tribunal must consider in determining the amount of the penalty (s. 95(5)).

Appeals to the Tribunal

The CPPA will also grant complainants and organizations a right to appeal before the Tribunal (s. 101) any decision issued by the Commissioner in which it finds that the organization has contravened, or not, the CPPA. This will also extend to any compliance order issued by the Commissioner against the organization and any decision issued by the Commissioner in which it decides not to recommend the imposition of a penalty. The decisions of the Tribunal are final and binding, subject only to a right to seek judicial review of the decision in Federal Court.

Offences

Certain more egregious conduct could constitute an offence leading to a fine of a maximum of the higher of C$25,000,000 and five per cent of the organization's gross global revenue in its previous financial year (s. 128). Such as for offences provided under section 28 of PIPEDA, these offences would be prosecuted by the Attorney General of Canada.

The following will constitute an offence under section 128 of the CPPA:

- Knowingly contravening the breach reporting and notification requirements (s. 58), including record-keeping requirements (s. 60(1));
- Knowingly contravening the requirement to retain personal information that is subject to an access request (s. 69);
- Knowingly using de-identified information to identify an individual (s. 75);
- Knowingly contravening a compliance order issued by the Commissioner; and
- Obstructing the Commissioner in the investigation of a complaint, in conducting an inquiry or in carrying out an audit.

Private right of action

The CPPA will introduce a new private right of action (s. 107). Individuals affected by a contravention of the CPPA may bring a claim against the organization for damages to compensate for loss or injury suffered due to that contravention, provided that:

- The Commissioner finds that the organization has contravened the CPPA and the finding may no longer be appealed, either because the time limit to appeal has expired or the Tribunal has dismissed a prior appeal; or
- The Tribunal finds that the organization has contravened the CPPA.

The CPPA also provides individuals with a private right of action against organizations convicted of an offence under the CPPA (*e.g.*, failing to report to the Commissioner, maintain records or certain information; penalizing an employee for reporting a CPPA contravention; or using de-identified information to identify an individual). Individuals affected by the act or omission of the organization which led to the conviction may bring a claim for the loss or injury suffered.

In each case, after a limitation period of two years after the date of the Commissioner's finding, the Tribunal's decision or conviction of a CPPA offence (as applicable) applies (s. 107(3)).

The private right of action under the CPPA appears to be considerably broader than the one introduced by Bill 64 in Québec, which is limited to an award of punitive damages of at least $1,000 when infringement is intentional or results from a gross fault.

Whistleblowing and anti-reprisal provisions

The CPPA maintains the whistleblowing protection that is currently included in PIPEDA (s. 126 CPPA replacing s. 27 PIPEDA). The Commissioner has used information received under this provision to initiate a complaint on at least one occasion (PIPEDA Case Summary #310). Similarly, the CPPA will also include an anti-reprisal provision which mirrors the one included in PIPEDA (s. 127 CPPA replacing s. 27.1 PIPEDA).

Codes of practice and certification programs

Sections 76 and 77 of the CPPA will bring in new provisions to enable the creation of "codes of practice" and "certification programs", a means of encouraging voluntary, sectoral practices that favour privacy protection. Similar provisions are included in Articles 40 to 43 of the GDPR and may provide for greater certainty in the application of the CPPA.

In order to further encourage the development of improved and consistent privacy practices, the CPPA will allow any organization, whether or not subject to the CPPA and including government institutions, to seek the Commissioner's approval of codes of practice and certification programs. Doing so will not necessarily be proof of compliance with the CPPA. However, the Commissioner has discretion to decline to investigate certified organizations (s. 83(1)(d)) and is prohibited from recommending that a penalty be imposed against an organization "if the Commissioner is of the opinion that, at the time of the contravention of the provision in question, the organization was in compliance with the requirements of [an approved] certification program (s. 93(3))". Organizations may choose to voluntarily comply and maintain certification as a means of reducing the risks associated with non-compliance with the CPPA and highlighting their committed to privacy compliance.

Accountability

Accountability - Summary of changes in C-27 from the previous version C-11 (2020)

- **Key change** → New power by the Commissioner to provide guidance on, or recommend that corrective measures be taken by the organization in relation to, its privacy management program. (s. 10(2))
- Sensitivity of personal information added as a factor for determining the length of the retention period. (s. 52(2))

In sections 7 through 11, the CPPA codifies and elaborates on the Principle of Accountability currently articulated in Schedule 1 of PIPEDA. While the changes to current requirements appear relatively limited, some notable additions under the CPPA will likely enhance the clarity of those requirements for businesses.

In light of Québec Bill 64, it is notable that the CPPA is silent about the obligation to conduct a privacy impact assessment in certain circumstances and a "privacy by design" requirement, both of which play an important role under the amended Québec privacy regime.

Notion of control

As under PIPEDA, the CPPA provides that an organization is accountable for personal information that is under its control (s. 7(1) CPPA replacing Principle 4.1 PIPEDA). However, the CPPA will go further by defining the notion of "control", stating that personal information "is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure" (s. 7(2) CPPA). Like PIPEDA, the CPPA reiterates that an organization has control over personal information even when the organization transfers the information to a service provider or where the information is collected, used or disclosed by a service provider on behalf of the organization (s. 7(2) CPPA replacing Principle 4.1.3 PIPEDA). Similarly to the GDPR, the CPPA distinguishes the obligations applicable to organizations in control and service providers, the latter not being subject to Part I of the Bill (which addresses obligations of organizations) except for section 57 (security safeguards) and section 61 (notification to customer in case of a breach).

Role of the privacy officer

The CPPA also echoes the PIPEDA requirement that an organization must designate an individual "to be responsible for matters related to its obligations" under the CPPA (s. 8 CPPA replacing Principle 4.1.1 PIPEDA) and provide the designated individual's business contact information to any person who requests it (s. 8 CPPA replacing Principle 4.1.2 PIPEDA). Unlike Québec Bill 64, which attributes this role to "the person exercising the highest authority" within the organization (*i.e.*, the CEO) by default, the CPPA does not specify who within the organization must fulfill this role.

Privacy management program

CPPA will require each organization to implement and maintain a "privacy management program" that includes (but presumably is not limited to) the policies, practices, and procedures the organization implements to fulfil its CPPA obligations. The required subject matter of these policies is generally the same as under PIPEDA: they must address the protection of personal information, the handling of inquiries and complaints, the training of staff on policies and procedures, and the development of materials to explain the policies and procedures (s. 9(1) CPPA replacing Principle 4.1.4 PIPEDA). Notably, the CPPA will introduce a new requirement that an organization, when developing its privacy management program, consider the volume and sensitivity of the personal information under its control (s. 9(2) CPPA). This is likely intended to reinforce the Commissioner's longstanding message that organizations' policies and safeguards need to be reasonable having regard to the types of information they handle.

The CPPA will also require that an organization give the Commissioner access to its policies, practices and procedures upon request (s. 10(1) CPPA). Although PIPEDA does not contain an equivalent requirement, organizations have generally provided such materials to the Commissioner in any event. The key change is that the CPPA adds that after reviewing such materials, the Commissioner may provide guidance on or recommend that corrective measures be taken (s. 10(2) CPPA).

Unlike Québec Bill 64, which requires organizations to publish detailed information about their internal policies and procedures on its website or, if the organization does not have a website, by any other appropriate means, the CPPA does not appear to impose a similar requirement with respect to its privacy management program.

Record of purposes

Additionally, section 12(3) of the CPPA will require an organization to identify and record each of the purposes for which it collects, uses, or discloses any personal information, and that it do so at or before the time of collection. In this respect, the CPPA appears to go beyond PIPEDA, which requires that organizations document only the purposes of collection (Principle 4.2.1 PIPEDA). If the organization determines that the personal information collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose (s. 12(4) CPPA).

Consent

Consent - Summary of changes in C-27 from the previous version C-11 (2020)

- Information to be provided in order to obtain consent must be provided in plain language that the individual would reasonably be expected to understand. (s. 15(4))
- Transparency (public-facing privacy policies): additional details to be included in readily available information about the organizations privacy management policies and practices: (i) description of activities in which they have a legitimate interest, and (ii) retention periods applicable to sensitive information. (s. 62(2)(b) and (e))
- Personal information of minors is sensitive information. (s. 2)
- **Key change** ➔ Consent exception for "business activities": Organizations may not rely on implied consent to collect or use personal information in the context of "business activities" – they may only rely on express consent or must satisfy the requirements set out in the "business activities" exception (s. 15(6)). "Business activities" no longer include activities carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk (s. 18(2)(b) and additional "business activities" may be created by regulation (s. 18(2)(d)). New legitimate interest consent exception and associated conditions, including an obligation to carry out and record a legitimate interest assessment. (s. 18(3), (4) and (5))
- Consent exception for fraud prevention, detection or suppression: The exception also applies to the use of personal information (not only to collection). (s. 27(2))
- **Key change** ➔ Business transactions: the condition to use de-identified information at the prospective business transaction stage is qualified and does not apply if it undermines the objectives of carrying out the transaction and the organization has taken into account the risk of harm to the individual that could result from using or disclosing the information. (s. 22(2))

The CPPA makes significant changes to the notion of consent by introducing a consent exception for specified business activities – initially proposed under C-11 (2020) – as well as a more flexible exception for certain processing operations carried out for the purpose of an activity in which the organization has a "legitimate interest". In addition, the CPPA (C-27) implements key recommendations made by the federal privacy commissioner in its submission on C-11 (2020), in particular by clarifying the need for objective standards for obtaining valid consent and requiring greater accountability for organizations wishing to rely on broader consent exceptions. In doing so, the CPPA moves away from the heavily criticized consent-centric model favoured by the current federal legislative regime to a more balanced approach that recognizes that consent is neither realistic nor reasonable in all circumstances. In short, 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.

The following summarizes some of the key provisions of the CPPA relating to the notion of consent and its exceptions, while highlighting the substantive changes made by C-27 as compared to PIPEDA and C-11 (2020).

Form of consent

Express consent remains the default form of consent under the CPPA, but an organization may rely on implied consent if doing so is "appropriate" in the circumstances, having regard to the "reasonable expectations of the individual" and the "sensitivity" of the personal information, neither of which, however, is explicitly defined in the legislation (s. 15(5) CPPA). Despite lacking a clear definition of the term "sensitive personal information", the personal information of "minors" – a notion defined according to the laws of each province – is deemed to be sensitive information (s. 2(2) CPPA), which, in turn, elevates the standard of consent (among other requirements) for this particular type of information. For other types of information, sensitivity will need to be assessed contextually (see the federal privacy commissioner's interpretation bulletin on sensitive information). It is also interesting to note that the federal government did not follow the Province of Québec's approach, which, as part of its privacy reform, opted to define the term "sensitive information" as information that, due to its nature, including medical, biometric or otherwise intimate information, or the context of its use or communication, entails a high level of reasonable expectation of privacy (s. 12 para. 4 (2) Bill 64).

Unlike C-11 (2020), C-27 introduces a potentially significant limitation on the notion of implied consent when processing is carried out in accordance with one of the new consent exceptions for specified or legitimate business activities under section 18 CPPA. In particular, section 15(6) CPPA appears to create a rule by which implied consent is deemed inappropriate if the collection or use of personal information is carried out for an activity falling within the scope of the new consent exception for specified business activities (s. 18(2)) or for activities in which the organization has a legitimate interest (s. 18(3)). These distinctions seem to strengthen the notion of consent by requiring organizations to rely on one of the consent exceptions noted above or to obtain express consent for one or more of the activities described in those provisions. However, given the breadth of activities potentially covered by the legitimate interest exception, it is unclear to what extent an organization can rely on implied consent without first undertaking a legitimate interest assessment in accordance with section 18(4) CPPA (as discussed in more detail below). We can expect the scope and application of section 15(6) CPPA to be clarified as C-27 progresses through the legislative process.

Privacy notice and informed consent

Regardless of the form of consent, an organization must provide the individual whose consent is sought certain types of information to ensure that their consent is sufficiently informed. Drawing from the federal privacy commissioner's *Guidelines for obtaining meaningful consent*, section 15(3) CPPA requires the following elements to be provided at or before the time their consent is sought:

- Purposes for which personal information is processed;
- Manner in which personal information is processed;
- Any reasonable foreseeable consequences resulting from the processing operations;
- Specific type of personal information that is to be processed; and
- Names or any third parties or types of third parties to which the personal information may be disclosed.

In line with the federal privacy commissioner's submission on C-11 (2020), section 15(4) CPPA now clarifies that the information described above needs to not only be provided in "plain language" but also in a language that is sufficiently adapted to the target audience such that it would be reasonable to expect them to "understand" the content of the notice. This is substantially in line with the requirement found under section 6.1 PIPEDA.

A key challenge that remains largely unresolved by C-27 is the actual manner and format in which this notice must be presented to an individual. For example, tools often used by organizations to present content in a convenient and accessible manner, such as layered and just-in-time notices, are not explicitly mentioned, despite the federal privacy commissioner's criticism that "[p]lain language information that is difficult to find, or presented in a format that makes comprehension difficult, does not lead to understanding (or meaningful consent)". While still lacking clear rules on format, content structure and accessibility of information, organizations must nevertheless consider the potential challenges resulting from the overall context in which consent is being sought when determining how to furnish or actively direct individuals to relevant information.

Withdrawal of consent and other key requirements

The CCPA largely maintains the *status quo* with respect to some of the other key consent-related requirements of PIPEDA. For example, consent to processing operations that are not necessary for the provision of a product or service cannot be a condition of service (**optionality of consent**); an individual is entitled to withdraw consent at any time, subject to reasonable notice and applicable law or the reasonable terms of a contract (**withdrawal of consent**); and, consent remains invalid if it was obtained by providing false or misleading information or using deceptive or misleading practices (**consent obtained by deception**).

New consent exceptions

Most consent exceptions found under PIPEDA are carried over to the CPPA with limited changes, if any. For example, PIPEDA reiterations include the exception for employment relationships (s. 24 CPPA replaces s. 7.3 PIPEDA), work product information (s. 23 CPPA replaces s. 7(1)(b.2) PIPEDA), and business transactions (s. 22 CPPA replaces s. 7.2 PIPEDA). The CPPA also introduces a number of new consent exceptions, including for certain specific business activities. As compared to C-11 (2020), however, the scope of the exception for specified business activities has been narrowed, but a new, more flexible consent exception has been introduced for activities in which an organization has a legitimate interest that "outweighs any potential adverse effect on the individual" resulting from the collection or use of their personal information. These exceptions, as well as a few others introduced specifically for de-identified information, are discussed in more detail below.

Specified Business Activity Exception. An organization may collect or use personal information without the individual's knowledge or consent if such processing is made for the purpose of a specified business activity, other than influencing the individual's behaviour or decisions, and falls within an

individual's reasonable expectations (s. 18(1) CPPA). In particular, the CPPA specifies that the following activities qualify as "business activities":

- The provision of a product or service that the individual has requested from the organization;
- The organization's information, system or network security;
- The safety of a product or service that the organization provides; or
- Any other activity prescribed by regulation.

As compared to C-11 (2020), however, the notion of "business activity" under C-27 no longer includes an activity "carried out in the exercise of due diligence to prevent or reduce the organization's commercial risks" or "in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual". These exceptions appear to have been removed in response to criticism from various stakeholders that their scope was too broad or unjustified.

Legitimate Interest Exception. A significant development is the inclusion of a new, flexible legitimate interest exception for collecting or using personal information without the individual's knowledge or consent. In particular, an organization may rely on this exception where personal information is collected or used for the purpose of an activity in which the organization has a (i) legitimate interest that outweighs any potential adverse effect on the individual resulting from the processing and (ii) does not involve influencing the individual's behaviour or decisions, and (iii) such processing falls within an individual's reasonable expectations (s. 18(3) CPPA).

In line with the privacy regulator's calls for greater authority to use personal information to be accompanied with greater accountability for organizations, an organization must, prior to relying on this exception, conduct and record a legitimate interest assessment ("**LIA**") and, on request, provide a copy of the assessment to the federal privacy commissioner. In particular, the LIA must:

- Identify any potential adverse effect resulting from relevant processing operations;
- Identify reasonable measures implemented to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and
- Demonstrate compliance with any other requirements prescribed by regulation.

While an organization that relies on this exception can collect and use personal information without an individual's knowledge and consent, it bears noting that an organization must nevertheless be transparent in its privacy policy about how it applies consent exceptions, including by providing a description of any activities falling within the scope of the legitimate interest exception (s. 62(2)(b) CPPA).

Although similar to the GDPR's notion of legitimate interest, the legitimate interest exception of the CPPA was likely modelled on Singapore's *Personal Data Protection Act* ("**PDPA**"), whose equivalent exception also remains embedded in a consent framework. In other words, the CPPA's legitimate interest exception is just that, an exception to the notion of consent, not an alternative and separate legal basis for processing data on an equal footing with consent. However, unlike under the PDPA and the GDPR, this exception does not apply to the disclosure of personal information to a third-party and does not explicitly permit consideration of the legitimate interest of another person (*i.e.* other than that of the organization collecting or using the information). In any event, it is not clear at this stage what specific types of activities might or might not fall within an organization's "legitimate interest" and, in particular, whether this might extend to

product improvement, the development of new products or services, or even certain forms of advertising or marketing, such as direct marketing or location-based advertising.

Specific Exceptions for De-Identified Information. In addition to permitting the use of personal information without knowledge or consent for de-identification (s. 20 CPPA), the CPPA offers organizations the following consent exceptions for de-identified information, which are, for the most part, consistent with what had been previously proposed under C-11 (2020), namely:

- **Socially Beneficial Purposes Exception.** An organization may disclose de-identified information to a government institution or other designated third parties if such disclosure is made for a "socially beneficial purpose", which relates to health, the provision or improvement of public amenities or infrastructure, the provision of the environment or any other purpose determined by regulation (s. 39 CPPA).
- **Internal Research, Analysis and Development Exception.** An organization may use de-identified information for its internal research, analysis and development purposes (s.21 CPPA).

While the CPPA continues to require parties to a prospective business transaction to de-identify personal information (among other requirements) in order to use or disclose such information without the individual's knowledge and consent (s. 22(1)), this requirement has been tempered. In particular, the organization is not required to de-identify the information prior to use or disclosure if doing so would undermine the objectives for carrying out the transaction and the organization has taken into account the risk of harm resulting from such processing (s. 22(2)).

Reasonableness test (appropriate purpose)

Reasonableness test (appropriate purposes) - Summary of changes in C-27 from the previous version C-11 (2020)

- Codification of case law specifying that an organization may collect, use or disclose personal information ***only in a manner*** and for purposes that a reasonable person would consider appropriate in the circumstances, ***whether or not consent is required***. (s. 12(1))

PIPEDA includes a catchall reasonableness test (*i.e.*, the "reasonable person" test), which dictates the limits of its application and which may apply even if consent was obtained from individuals. The CPPA includes a similar requirement under which an organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances (s. 12(1) CPPA replacing s. 5(3) PIPEDA). While this provision of the CPPA under C-27 is similar to the one provided under PIPEDA and C-11 (2020), the wording "in a manner" was added in C-27 and the new bill also specifies that this reasonableness test applies "whether or not consent is required under this Act".

The CPPA provides the factors that must be taken into account in determining whether the manner and the purposes are appropriate. These factors are largely the same as those elaborated in the *Turner v. Telus Communications Inc.* decision in which the Federal Court, and subsequently affirmed by the Federal Court of Appeal, set out the factors for evaluating whether an organization's purpose was in compliance with subsection 5(3). These factors are:

- The sensitivity of the personal information;
- Whether the purposes represent legitimate business needs of the organization;
- The effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;
- Whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
- Whether the individual's loss of privacy is proportionate to the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual (s. 12(2) CPPA).

Since the wording of the new provision is similar to the one used under PIPEDA, the *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* document published by the Commissioner in May 2018 may still be relevant.

As discussed above (see "Record of purposes" in Accountability section), under the CPPA, at or before the time of the collection of personal information, each of the purposes for which the information is to be collected, used or disclosed must be determined and recorded (s. 12(3) and (4) CPPA).

While Québec's Bill 64 doesn't include a similar reasonableness test, in analyzing the necessity of the collection of personal information under section 5 of Québec Private Sector Act, the Québec Commission d'accès à l'information evaluates whether the objective is important, legitimate and real, and the proportionality between the objective and the invasion of privacy (*Institut généalogique Drouin Inc.*, CAI 091570, decision of D. Poitras, February 6, 2015).

Individual rights

Individual rights - Summary of changes in C-27 from the previous version C-11 (2020)

- **Key change** ➔ Individual rights do not apply to de-identified information (s. 2(3)), there are new conditions for the right to disposal (s. 55(1)) and new exceptions to the right to disposal (s. 55(2)).
- **Key change** ➔ Automated decision-making: the requirement to provide an explanation regarding automated decision-making only applies to a prediction, recommendation or decision that could have a significant impact on the individual (s. 63(3)).
- **Key change** ➔ Right to disposal: new conditions (s. 55(1) and new exceptions (s. 55(2) to the right of disposal.

As with PIPEDA, the CPPA will grant individuals the right to access and amend their personal information. The CPPA will also provide individuals with new rights relating to automated decision-making, data disposal and data mobility under specified circumstances. Interestingly, the CPPA expressly excludes personal information that has been de-identified from some – but not all – of the individual rights set out in the CPPA.

Right to access and amend

Sections 63 to 71 of the CPPA set out the individual rights to access and amend personal information. Subject to the limited exceptions set out below, the CPPA's access and amendment provisions will not deviate from the previous regime set out in PIPEDA (ss. 8 and 9 and Principle 4.9 PIPEDA).

Information about retention, use and disclosures to third parties. As with PIPEDA, after receipt of a written request by an individual, an organization must inform the individual in plain language: whether the organization holds any personal information about the individual, how the organization uses the personal information and whether the organization has disclosed the information; and to the extent the personal information has been disclosed, the names of the third parties or types of third parties to whom the disclosure was made (including when such disclosure was made without consent). With respect to the latter information disclosure, PIPEDA allows an organization to provide an individual with a list of third parties to which it *may* have disclosed the individual's personal information if it is not possible to provide an accurate list of third parties to which disclosure was made – an option that is notably absent from the CPPA (ss. 63(1) and (2) CPPA replacing Principle 4.9.3 PIPEDA).

Amendments to personal information. As with PIPEDA, if an organization grants an individual access to their personal information and the individual demonstrates that their personal information is inaccurate, outdated or incomplete, the CPPA will require the organization to amend the individual's personal information and to provide the amended personal information to any third party that has access to the personal information. If the organization disagrees with the individual about the requested amendments, the organization must keep a record of the disagreement and inform third parties that have access to the personal information about the disagreement (ss. 71 and 71(3) CPPA replacing Principles 4.9.5 and 4.9.6 PIPEDA).

Retention of personal information used for decision-making. As with PIPEDA, the CPPA will require an

organization that uses personal information to make a decision about an individual to retain the information for a period of time that is sufficient to permit the individual to make a request for access (s. 54 CPPA replacing Principle 4.5.2 PIPEDA). An organization that has personal information about an individual subject to a request by the individual about how the organization holds, uses and discloses the personal information must retain the information for as long as is necessary to allow the individual to exhaust all recourse available under the CPPA (s. 69 CPPA replacing s. 8(8) PIPEDA). The CPPA sets this retention period at six months from the date of the refusal to grant the request (or failure to respond to such request), but the Commissioner can decide to extend this period (ss. 54 and 82(3) CPPA).

Right to be informed of automated decision-making systems

The CPPA will grant a new right for an individual to receive an explanation about the use of an automated decision system to make a prediction, recommendation or decision about the individual that could have a significant impact on them – an individual right reflected in both Québec Bill 64 and the GDPR but not PIPEDA (s. 63(3) CPPA). Contrary to Québec Bill 64 and the GDPR, however, the CPPA's automated decision-making provisions do not extend to permitting individuals with the right to object to such use or to have the decision reviewed by an employee of the organization (for more information on the CPPA's provisions regarding automated decision-making systems, see section entitled "De-identification, research and analytics" below).

Right to disposal

Section 55 of the CPPA will establish a new right for an individual to request that an organization dispose of (*i.e.*, permanently and irreversibly deletes) their personal information under the organization's control and according to conditions newly introduced under C-27, such as if: (a) the organization collected, used or disclosed the personal information in contravention of the CPPA; (b) the individual has withdrawn their consent to the organization's collection, use or disclosure of the personal information; or (c) the personal information is no longer necessary for the continued provision of a product or service to the individual.

The CPPA permits the organization to refuse a disposal request under certain circumstances, including if the disposal would result in the disposal of personal information about another individual and the information is not severable, a contractual or legal requirement prohibits the disposal, the disposal would have an undue adverse impact on the ongoing provision of a product or service to the individual, the individual's request was vexatious or made in bad faith or – significantly – the information is scheduled to be disposed of in accordance with the organization's retention policy and the organization informs the individual of the remaining time period for which the information will be retained. Many of these circumstances to justify refusing a disposal request were not included in C-11 (2020) and have been added in C-27.

Notably, the CPPA's right to disposal does not appear to include a right to de-indexation or right to be forgotten, unlike Québec Bill 64 and the GDPR.

Right to mobility

The CPPA will innovate at section 72 by creating a limited right to data portability, which will allow individuals to request that an organization disclose to a third party organization designated by the individual information that the first organization has collected from the individual, provided that both organizations are subject to a "data mobility framework" (to be prescribed by regulations under the CPPA). Importantly, the mobility right extends only to personal information that the organization collects from individuals (*i.e.*, not from third parties). The CPPA provides that the regulations may establish safeguards for the secure disclosure of information and parameters for the technical means for ensuring interoperability (s. 123 of CPPA). The regulations may also specify certain organizations subject to the framework, which seems to suggest that the CPPA's mobility right may be limited to specific industry sectors (such as banking and telecommunications). Of note, the CPPA's mobility right will be more limited in scope than Québec Bill 64 and the GDPR because of the restrictions on which organizations may be subject to data portability requests. As a result, the CPPA does not fully open the door to permit the general portability requests found in each of Québec Bill 64 and the GDPR.

A caveat: de-identified information and individual rights

Interestingly, the CPPA introduces a new caveat to certain of the individual rights. Appearing to acknowledge the commercial difficulty that organizations can face in re-identifying de-identified information to comply with their privacy law obligations, the CPPA provides that personal information that has been de-identified will *not* be considered personal information for the purposes of the right to disposal, the right to access and amend, and the right to data mobility (s. 2(3) CPPA)). The right to be informed of automated decision-making systems still applies to de-identified information.

De-identification, research and analytics

De-identification, research and analytics - Summary of changes in C-27 from the previous version C-11 (2020)

- **Key change** ➔ Revised definition of "de-identify": "means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains." (s. 2)
- **Key change** ➔ New definition of "anonymize": "means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means." (s. 2)
- **Key change** ➔ Explicit recognition that the CPPA does not apply in respect of personal information that has been anonymized (s. 6(5)) and additional exceptions to the prohibition on re-identifying de-identified information (s. 75)
- An organization may request the Commissioner's authorization to re-identify an individual based on de-identified information, if the Commissioner believes it is clearly in the interests of the individual (s. 116)
- The consent exception regarding de-identified information for research and development purposes extends to analysis. (s. 21)
- **Key change** ➔ The consent exception allowing disclosure of personal information is no longer limited to "scholarly" study or research purposes. (s. 35)

The CPPA introduces definitions for the terms "anonymize" and "de-identify", and a set of circumstances in which de-identified information will not be considered personal information. This will allow organizations to benefit from greater flexibility with respect to processing such de-identified information, including for internal research and analytics purposes.

De-identification and anonymization

The draft CPPA, in sharp contrast to the earlier proposed legislation introduced under Bill C-11 (2020), introduces a clear separation between de-identified information and anonymized information. Under the CPPA, to "de-identify" will mean "to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains" (s. 2). To "anonymize" will mean "to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means" (s. 2). In this respect, the CPPA approach aligns quite closely with Québec's Bill 64, which introduced similar distinctions. While there are some differences with the definitions coming into force under Québec's privacy law framework, there are certain essential similarities that bode well for harmonization in approach and interpretation by Canadian privacy regulators. For example, in both cases, de-identification

is focused on the elimination of direct identifiers, and anonymization on the irreversible transformation of personal information into information that no longer identifies an individual, whether directly or indirectly.

Importantly, the CPPA provides that the act of de-identifying personal information is a use of personal information that does not require the knowledge or consent of individuals (art. 20). The CPPA also provides that anonymization is considered a form of disposal (s. 2(1)), and organizations have a standing obligation to dispose of personal information when it is no longer necessary to fulfil the purposes for which it was collected, use or disclosed or to comply with applicable laws (s. 53(1)). In consequence, the CPPA provides a framework that permits organizations to de-identify or anonymize personal information without needing to obtain specific consent to do so, resolving a long-standing ambiguity under PIPEDA.

The relatively undemanding threshold chosen for de-identification – the removal of directly identifying information – makes it possible for organizations to preserve the richness of record-level data essential for internal research. However, the CPPA will contain certain measures that must be taken, and certain restrictions that apply, in connection with handling de-identified personal information. Section 74 states that an organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information. Section 75 states that an organization must not use de-identified information alone or in combination with other information to identify an individual, except in order to: (a) conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information; (b) to comply with any requirements under the CPPA or under federal or provincial law; (c) to conduct testing of the fairness and accuracy of models, processes and systems that were developed using information that has been de-identified, (d) to conduct testing of the effectiveness of its de-identification processes, and for other authorized or prescribed circumstances. Moreover, organizations that knowingly contravene section 75 are liable to a fine of up to the higher of $25,000,000 or five per cent of the organization's gross global revenue (s. 128(a)). These sections implicitly recognize the inherent risk of re-identification associated with forms of de-identified data, and seek to strike a balance between its use and the protections / restrictions that should be in place in order to minimize that risk.

Of great significance in contrast to the earlier version of the CPPA is the introduction of an interpretative framework for de-identified information that sets out circumstances in which it is not considered personal information. CPPA section 2(3) states: "[f]or the purposes of this Act, **other than** sections 20 and 21, subsections 22(1) and 39(1), sections 55 and 56, subsection 63(1) and sections 71, 72, 74, 75 and 116, personal information that has been de-identified is considered to be personal information" (emphasis added). Review of these exceptions discloses a carefully considered framework that addresses several challenges related to treating de-identified information in the same way as more canonical forms of personal information. For example, obligations for organizations to dispose of personal information upon individual request (CPPA s. 55), maintain its accuracy (s. 56), provide access to it or amend it upon request (s. 63(1) and 71(1) CPPA), are all inapplicable to de-identified information. Collectively, these provisions create a fairly compelling incentive for organizations to de-identify personal information before using it for research and development (rather than seeking consent to use personal information in its native state), by rendering inapplicable many of the obligations that would be difficult to put into practice for de-identified data.

Finally, we note that the CPPA does not apply to personal information that has been anonymized (s. 2(5) CPPA).

Research

The CPPA will introduce a new consent exception that will allow the use of personal information for an organization's internal research and development purposes, if the information is de-identified before it is used (s. 21 CPPA). Similar to the amendments introduced by Québec's Bill 64, the CPPA thereby will permit organizations to re-use information collected for one purpose for secondary research purposes, such as enterprise or business analytics. The amendments made to section 75 also confirm what we had suspected would be the case with respect to using de-identified data for machine learning, namely that such information to train machine learning systems will arguably also fall within the "research and development" contemplated by this exception.

Automated decision systems and AI

In this section, we discuss the provisions governing automated decision systems in the context of the CPPA, both as a function of the internal logic of the CPPA as well as potential interactions with certain provisions of the new *Artificial Intelligence and Data Act* ("AIDA"). We will address AIDA in-depth in a separate article.

We note at the outset that the key defined terms as between the CPPA and AIDA overlap but are definitely not coterminous. The CPPA defines "automated decision systems" as "technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique" (CPPA s.2). AIDA instead concerns itself with the notion of "artificial intelligence system," defined as "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions" (AIDA s. 2). These differences in scope are not surprising, given that the CPPA seeks to address the accuracy of decisions rendered by automated decisions systems that make use of personal information, and AIDA is concerned with the wider risks to individual rights that the use of AI systems presents.

There are also potential differences in jurisdiction as between the two proposed laws, given that the CPPA is intended to apply to intra-provincial matters to the extent that no substantially similar provincial law has been declared by regulation (CPPA s. 122(3)), and AIDA appears to only expressly apply to activities carried out in the course of international or interprovincial trade and commerce (AIDA s. 5(1)).

Despite these differences in scope and jurisdiction, significant potential for overlap remains and in certain circumstances CPPA obligations may be displaced by the more stringent obligations of AIDA, as discussed below. The CPPA will invoke automated decision systems in three contexts, "Openness and Transparency" (s. 62 CPPA), "Access to and Amendment of Personal Information" (s. 63-71 CPPA), and in the context of restrictions on the use of de-identified data (s. 75).

Openness and Transparency

Under Openness and Transparency, an organization using an automated decision system will be obliged 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 (s. 62(2)(c) CPPA). The phrase "significant impact" is not defined or elucidated. One natural interpretation could include some of the circumstances that may give rise to "significant harm" as that term is defined under section 58(7) of the CPPA, such as circumstances involving reputation, employment, finances or credit.

However, organizations will also need to pay attention to future elucidation of the term "high-impact system" as this term is used in AIDA. The criteria for high-impact systems will be established in regulations (AIDA s. 5(1)). The use of high-impact systems carry transparency obligations as well, which go beyond the requirements under the CPPA for the automated decision systems that could have a significant impact. Instead of a general account, users of high-impact systems will need to publish a plain-language description that includes an explanation of how the system is used, the types of content it generates and the decisions, recommendations or predictions that it makes, the mitigation measures established to address the risks of

harm or biased output created by the use of the system, and any other information prescribed by regulation (AIDA s. 11(2)). Meeting the transparency obligations of AIDA while not disclosing confidential business information (although we note that AIDA is very much alive to this concern and has provisions in place to address it (AIDA ss. 5(1), 18(1), 22-29) or information that would allow unauthorized third party to game such systems will likely be challenging given the level of specificity required.

In consequence, given the obvious opportunity for interaction between the two proposed laws, it appears that the legislators intend to set up a distinction between significant impact and high-impact systems, with the greater transparency obligations of high-impact systems that also fall within the definition of automated decision systems under the CPPA.

Access to and Amendment of Personal Information

Under Access to and Amendment of Personal Information, if an organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization will be required, on request by the individual, to provide them with an explanation of the prediction, recommendation or decision (s. 63(1)(3) CPPA). The explanation must indicate the type of personal information that was used to make the prediction, recommendation or decision, the source of the information and the reasons or principal factors that led to the prediction, recommendation or decision (s. 63(4) CPPA). These provisions of the CPPA setting out the content of the explanation have been amended from the antecedent versions set out in C-11 (2020), and brings them into very close alignment with the provisions of Québec's Bill 64.

The elucidation of the main components of the obligation to explain is a helpful advance on the previous version, but may yet be rendered challenging by the additional requirement set out in CPPA section 66(1), which obliges the organization to provide this information to the individual in plain language. Whereas the plain language requirement set out in the provisions governing openness and transparency will be satisfied by giving "a general account", it is not clear whether a plain language explanation of a given prediction, recommendation or decision can be given when the system used is based on machine learning, deep learning or neural network.

The CPPA does not provide individuals with any further rights beyond the right to an explanation. For example, in contrast to Québec's Bill 64, individuals can submit observations to a designated person within the organization that is in a position to review the decision. Moreover, the CPPA provisions that will permit individuals to have information amended if they can demonstrate that the information is not accurate, up-to-date or complete (s. 71(1) CPPA) do not provide a clear foundation for challenging the conclusions reached by an automated decision system.

Re-identification

The CPPA introduces an interesting exception to the general prohibition on deliberately using de-identified personal information to re-identify an individual. Section 75(c) CPPA states that de-identified information can be used to identify an individual to "conduct testing of the fairness and accuracy of models, processes and systems that were developed using information that has been de-identified." The reference to "models" is almost certainly meant to refer to the output of the process of machine learning: the trained result is routinely referred to as a "model" in AI literature. So interpreted, CPPA section 75(c) dovetails with the obligations set out in AIDA for persons responsible for high-impact systems, to assess and mitigate risks of harm or biased output.

Testing machine learning models that will be used in high-impact systems for such risks of harm or bias would therefore not be impeded by reidentification risks, where these arise because the training data used was de-identified. It remains to be seen, however, whether the inclusion of the exception to the general prohibition on re-identification will be interpreted by regulators as implying that such testing for fairness and accuracy should be undertaken on all models, processes and systems, whether or not they meet the criteria for high-impact system to be articulated in AIDA's regulations.

Outsourcing and cross-border

Outsourcing & cross-border transfers - Summary of changes in C-27 from the previous version C-11 (2020)

- Organizations must ensure that service providers provide a level of protection ***equivalent*** to that which the organization is required to provide under the Act (rather than ***substantially the same protection***) (s. 11(1))

The CPPA will not materially change outsourcing or cross-border requirements. Rather, it will formally incorporate existing requirements and best practices, and clarify the roles and obligations of an organization that has personal information under its control and its service providers. In addition, the CPPA will confirm that service providers that use personal information for their own purposes must comply with all CPPA requirements regarding the collection, use and disclosure of the information. For businesses, these changes will likely be welcome in that they will provide greater clarity and consistency.

Outsourcing

The CPPA provides welcome clarity with respect to the transfer of personal information to a service provider, which the CPPA defines as "an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes" (s. 2).

Section 19 of the CPPA confirms that organizations may transfer an individual's personal information to a third party service provider without the individual's knowledge or consent, which will provide a definitive conclusion to a tumultuous few years in which the Commissioner adopted, and subsequently reversed, a policy position that the transfer of personal information for processing required additional, express consent.

The CPPA also elucidates the following principles and requirements for outsourcing arrangements that involve personal information:

- The CPPA deems personal information collected, used or disclosed on behalf of an organization by a service provider to be under the control of the organization (not the service provider) if the organization decides to collect the information and determines the purposes of collection, use or disclosure (s. 7(2));
- As with PIPEDA, the CPPA requires an organization that transfers personal information to a third party service provider to "ensure (by contract or otherwise) that the service provider provides a level of protection of the personal information equivalent to that which the organization is required to provide" under the CPPA (s. 11(1));
- The CPPA clarifies that most of the obligations set out in Part 1 of the CPPA do not apply to a service provider in respect of personal information transferred by another organization to the service provider for processing. However, a service provider will be subject to all obligations set out in Part 1 of the CPPA if the service provider collects, uses or discloses personal information transferred by another organization for any purpose other than the purposes for which the information was transferred (s. 11(2));

- The CPPA confirms that service providers must protect personal information through physical, organizational and technological security safeguards that are proportionate to the sensitivity of the information (s. 57);
- If an organization disposes of personal information at an individual's request, then the organization must, as soon as feasible, inform each service provider to which the organization transferred the information and ensure that the service provider has disposed of the information (s. 55(4)); and
- A service provider that suffers a breach of security safeguards must as soon as feasible notify the organization that controls the personal information (s. 61; see the "Safeguarding and incident response" section for more information).

It is also worth noting, by way of comparison, that Québec Bill 64 incorporates similar requirements with respect to outsourcing, although its requirements with respect to the content of outsourcing agreements are more prescriptive than under the CPPA.

Cross-border transfers and cooperation

Section 6(2) of the CPPA confirms that the CPPA applies in respect of personal information that is collected, used or disclosed interprovincially or internationally.

Contrary to Québec Bill 64 and the GDPR, which provide for an evaluation of the foreign privacy framework's level of equivalency, but in line with PIPEDA and past guidance from the Commissioner, the CPPA does not contain any restriction to the transfer of personal information outside of Canada.

Transparency. The only requirement found in the CPPA at section 62(2)(d) is a transparency one: the privacy statement to be made available by organizations will have to include details as to whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information but only if the transfer or disclosure may have "reasonably foreseeable privacy implications". This last portion of the requirement is unclear and seems to imply that the transparency statement must only be made where personal information is shared with an organization/entity that might be subject to foreign legal disclosure obligations (*i.e.*, which cannot be prohibited by contract) that are not substantially similar to those applicable in Canada.

Cooperation with foreign regulators. Acknowledging the inherent international nature of data protection efforts, section 120 of the CPPA will afford the Commissioner new powers regarding the disclosure of certain information to foreign privacy regulators. Interestingly, the powers will include the ability to enter into cooperation agreements with foreign regulators, which may involve: cooperation for enforcing data protection laws and the handling of complaints; developing guidance, standards and other documents regarding the protection of personal information; undertaking and publishing research; sharing knowledge and expertise; and identifying issues of mutual interest.

Safeguards and incident response

Safeguards and incident response - Summary of changes in C-27 from the previous version C-11 (2020)

- Security safeguards include "reasonable measures to authenticate the identity of the individual to whom the personal information relates" (s. 57(3))

The CPPA will include a security-safeguarding obligation that is very similar to that now in effect under PIPEDA – an obligation to protect personal information through "proportionate" physical, organizational and technological security safeguards (s. 57(1) CPPA). Sensitivity will become the new primary factor governing the adequacy of security safeguards, though "the quantity, distribution, format and method of storage of the information" will continue to be relevant (s. 57(2) CPPA).

The new bill C-27 specifically addresses authentication. An organization's safeguards will need to include reasonable measures "to authenticate the identity of the individual to whom the personal information relates" (s. 57(3)). We note that the notion of "identification" which means finding an identity in a database to determine who the person is (whereas "authentication" consists of verifying or confirming the identity of an individual) was not included in this new requirement. Thus, the CPPA emphasizes on implementing technical, organizational and physical measures that would be considered "reasonable" in order to verify or confirm if the individual is who he claims to be. To this end, organizations should pay attention to the risk of fraud and identity theft when assessing the appropriate safeguards to put in place to protect the personal information of the individuals they authenticate, and consider implementing information security best practices.

The CPPA will preserve the notification and reporting requirements that apply to "breach of security" safeguards as they exist today. Namely:

- The "breach of security safeguards" definition is unaltered, and continues to include the "loss of, unauthorized access to or unauthorized disclosure of personal information" (s. 2);
- The CPPA will continue to require reporting to the Commissioner and individual notification (ss. 58(2), 58(3));
- The standard for reporting and notification will continue to be the "real risk of significant harm" standard (ss. 58(1), 58(7), 58(8));
- The time requirement for reporting and notification will continue to be "as soon as feasible" after the breach has occurred (s. 58(6)); and
- There will continue to be a requirement to notify other organizations who are believed to have an ability to reduce the risk of harm or mitigate harm (s. 59).

The only new requirement is that a service provider will be obligated to notify its customer organizations that control personal information "as soon as feasible" after determining that a breach of security safeguards involving the personal information has occurred (s. 61). This change will establish a statutory minimum for service provider notification, a matter typically governed by the terms of service provider agreements. The trigger for notification – a determination that a breach of security safeguards involving personal information has occurred – will give the service provider time to investigate security incidents before giving notice.

Next steps

It is notable that the employees of Innovation, Science and Economic Development Canada have indicated during a technical briefing following the tabling of Bill C-27, that businesses should expect a significant transition period between the adoption of the bill and its coming into force. Also, since the proposal contemplates a considerable increase in penalties, it is likely that the government will hold consultations and hearings in order to obtain the input of stakeholders, as was recently the case in Québec with respect to Bill 64 (see "*Summary of special consultations and public hearings on Québec's Bill 64*" for more detail).

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

Authors

Sep Alavi
T 604.632.3472
salavi@blg.com

Eric Charleston
T 416.367.6566
echarleston@blg.com

Simon Du Perron
T 514.954.2542
SDuperron@blg.com

Daniel-Nicolas El-Khoury
T 514.954.2555
delkhoury@blg.com

Bradley Freedman
T 604.640.4129
bfreedman@blg.com

Julie Gauthier
T 514.954.2555
jugauthier@blg.com

Roberto Ghignone
T 613.369.4791
rghignone@blg.com

Eloïse Gratton
T 416.367.6225
egratton@blg.com

Anthony Hémond
T 514.395.3899
ahemond@blg.com

Elisa Henry
T 514.954.3113
ehenry@blg.com

Max Jarvie
T 514.954.2628
mjarvie@blg.com

François Joli-Coeur
T 514.954.3144
fjolicoeur@blg.com

Dan Michaluk
T 416.367.6097
dmichaluk@blg.com

Shane Morganstein
T 416.367.7281
smorganstein@blg.com

Catherine Labasi-Sammarito
T 514.954.2555
clabasiSammartino@blg.com

Andy Nagy
T 514.395.2714
anagy@blg.com

Katherine Stanger
T 416.367.7294
kstanger@blg.com

Danielle Windt
T 604.640.4120
dwindt@blg.com