# STANDING COMMITTEE ON RESOURCE STEWARDSHIP

LEGISLATIVE ASSEMBLY OF ALBERTA

# Emerging Issues:

# The *Personal Information Protection Act*

Prepared by:
Legislative Assembly Office
Research Services
February 13, 2024

## Table of Contents

## List of Tables

## 1.0 Introduction

Alberta's *Personal Information Protection Act* (PIPA) came into effect on January 1, 2004. PIPA includes provisions protecting the personal information of private sector organizations' customers, clients, and employees. Its rules on collecting, using, and disclosing personal information attempt to balance:

- an individual's right to have their personal information protected and
- an organization's need to collect, use, or disclose personal information for reasonable purposes.

The Act requires that a special committee of the Legislative Assembly review the Act every six years. Previous statutory reviews took place in 2006-2007 and 2015-2016.

On December 5, 2023, Government Motion 9 was agreed to by the Assembly. This motion designated the Standing Committee on Resource Stewardship as a special committee of the Assembly for the purpose of conducting the current comprehensive review of PIPA. The Committee must report to the Legislative Assembly within 18 months of the beginning of its review. The Committee's first meeting occurred on January 22, 2024.

At a meeting on January 22, 2024, the Committee passed a motion directing Research Services

> to prepare a document identifying emerging issues related to the Personal Information Protection Act, including issues related to proposed federal legislation currently under consideration by the House of Commons in Bill C-27, *Digital Charter Implementation Act*, 2022.

### 1.1 How to use this Document

This document outlines some emerging issues related to privacy that may be useful to consider in the review of PIPA. Each emerging issue is summarized and includes questions that may help guide the discussion.

Should it choose, the Committee may wish to distribute this document during its call for submissions as the issues included here, although not exhaustive, may be helpful for both stakeholders and committee members alike.

### 1.2 Emerging Issues Derived from Changing Legislative and Technological Landscape

The legislative landscape in Canada and internationally has significantly changed since the enactment of PIPA in 2004. The emerging issues identified in this document derive from a high-level comparison of this changing legislative landscape.[*] This document summarizes the following issues and topics:

- the changing legislative landscape in Canada and internationally
- the changing digital economy, particularly the use of artificial intelligence and the potential need to regulate its design, development, and use
- the application of PIPA to non-profit organizations and political parties
- protections of sensitive personal information
- individual rights that are not included under PIPA
- safeguarding personal information
- breach notifications
- administrative monetary penalties.

[*] This document includes only select high-level cross-jurisdictional information. A comprehensive cross-jurisdictional comparison is also provided to the Committee by the Legislative Assembly Office.

## 2.0 The Changing Legislative Landscape in Canada and Internationally

The technological change since the enactment of PIPA in 2004 has created new business opportunities relating to the transaction of personal information. Personal information in and of itself is now a part of trade, and this brings new challenges for protecting personal privacy.

In some jurisdictions, new legislation attempts to protect individuals' personal information. Most notably, the European Union's *General Data Protection Regulation* (hereafter GDPR), enacted in May 2018, is considered the international gold standard for privacy legislation. Furthermore, the governments of British Columbia, Quebec, and Canada have recently enacted or are considering amendments to private-sector privacy legislation in their jurisdictions.

### 2.1 Existing Canadian Legislation and Proposals for Change

The access and privacy landscape in Canada includes several pieces of legislation:

#### 2.1(a)Canada

Federal works and undertakings, and private sector organizations in provinces without "substantially similar" provincial legislation, are subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). This Act also applies when private-sector organizations transfer personal information across borders.

Bill C-27, *Digital Charter Implementation Act* (DCIA), received second reading on April 24, 2023, and is currently under consideration by the House of Commons Standing Committee on Industry and Technology.[*] Bill C-27 proposes substantial changes to PIPEDA:

- modernize private sector privacy legislation in Canada such that it is more responsive to changes in technology
- bring federal private sector privacy legislation more in line with the European Union's General Data Protection Regulation (GDPR)

It is a requirement for Canadian businesses to comply with the GDPR if they are seeking access to markets within the European Union and/or processing the personal information of individuals (not just residents) located in the European Union.

Bill C-27 proposes to repeal and replace the provisions of PIPEDA that deal with protecting personal information in the private sector.

1. The *Consumer Privacy Protection Act* (CPPA) is the Bill's centrepiece. The CPPA sets out new rules governing collecting, using, and disclosing personal information for commercial activity in Canada. In addition, the CPPA seeks to balance the right of an individual's privacy with respect to their personal information and the need of organizations to collect, use or disclose personal information while carrying out business activities.

2. In addition, Bill C-27 proposes establishing a Personal Information and Data Protection Tribunal to hear appeals of certain decisions made by the federal Privacy Commissioner under the CPPA. It also proposes administrative monetary penalties for specific violations.

[*] Canada, House of Commons, *Digital Charter Implementation Act*, LegisInfo, https://www.parl.ca/LegisInfo/en/bill/44-1/c-27 [accessed January 31, 2024].

3. Finally, Bill C-27 includes the *Artificial Intelligence and Data Act* (AIDA), which proposes to regulate international and interprovincial trade and commerce in artificial intelligence systems by requiring measures to mitigate risks of harm.[*]

### 2.1(b) Alberta

Alberta has the *Personal Information Protection Act* (PIPA), which the Privy Council designated as "substantially similar" to PIPEDA on October 12, 2004. This designation means private sector organizations collecting, using, or disclosing personal information in Alberta are subject to Alberta PIPA, not PIPEDA.

### 2.1(c) British Columbia

British Columbia also has a *Personal Information Protection Act*, which the Privy Council designated as "substantially similar" to PIPEDA on October 12, 2004.

British Columbia's Special Committee to Review the Personal Information Protection Act reported to the Legislative Assembly of British Columbia in December 2021. The Committee's final report, *Modernizing British Columbia's Private Sector Privacy Law*, included 34 recommendations. In its final report, British Columbia's Special Committee to Review the Personal Information Protection Act stressed the importance of harmonization with the changing federal, provincial, and international privacy landscape, including the European Union's GDPR. Members also focused on new provisions for the rapidly changing digital economy and recommended changes to BC PIPA to reflect modern information processing practices and their impact on privacy.

Changes to British Columbia's PIPA based on the Committee's recommendations have yet to be enacted.

### 2.1(d) Quebec

Quebec *has Loi sur la protection des renseignements personnels dans le secteur privé/An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c. P- 39.1 (QSPA), which the Privy Council designated as "substantially similar" to PIPEDA on November 19, 2003.[†]

On September 22, 2021, the Quebec government adopted Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, which amended QPSA. Provisions of Bill 64 come into force between 2021 and 2024.

Key amendments to QPSA include

- the creation of a person in charge of protecting personal information within an enterprise
- requirement that people operating an enterprise ensure that any technological products or services they use provide the highest level of confidentiality by default
- individuals' information included on nominative lists must consent to being contacted for commercial and philanthropic purposes
- individuals have the right to de-indexation[‡]

---

[*] House of Commons of Canada, Bill C-27, available at https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading (accessed September 15, 2022).

[†] National Assembly of Quebec, Bill 64, *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information*, which included significant proposed amendments to an *Act Respecting the Protection of Personal Information in the Private Sector*, available at http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html (accessed September 6, 2022).

[‡] Quebec's de-indexation is similar to the GDPR's right to be forgotten. Specifically, de-indexation enables an individual to require an enterprise to cease disseminating personal information or to de-index any hyperlink that involves access to specific information about that individual by a technological means when disseminating this information violates a law or court order. In sum, it allows for the suppression of search results that violate a law or court order (rather than the deletion of the online content itself).

- empowerment of the Commission d'accès à l'information to impose monetary administrative penalties

### 2.2 The General Data Protection Regulation

The *General Data Protection Regulation* (GDPR) came into effect on May 25, 2018, and directly applies to European Union member states. The purpose of the GDPR is to protect data belonging to individuals located in the EU. The GDPR harmonizes data privacy laws across Europe, gives improved privacy protection and rights to individuals, and extends the reach of personal data protection beyond the borders of the EU.

Compliance with the GDPR is necessary for business transactions within the European Union (EU) and businesses that handle data belonging to individuals in the EU. The law applies to organizations that process personal data regardless of location: this is the "extra-territorial effect."[*]

As noted, the GDPR is the international gold standard for privacy legislation. Many of the provisions of Quebec's amended QPSA align with the provisions of the GDPR. Furthermore, British Columbia and the Government of Canada are considering proposals to change their private sector privacy legislation to align the statutes in each jurisdiction more closely with the GDPR.

Canadian organizations must comply with the GDPR if they:[†]

- have an established presence in the EU;
- offer goods and services to individuals in the EU; or
- monitor the behaviour of individuals in the EU.[‡]

The GDPR applies to organizations that have an established presence in the EU, offer goods and services to individuals in the EU, or monitor the behaviour of individuals in the EU. Organizations that do not comply with the GDPR face significant fines. There are two tiers of penalties, whose maximum is €20 million or four per cent of global revenue (whichever is higher), and data subjects (individuals) have the right to seek compensation for damages.[§]

**Questions**

**1. Are there specific amendments needed to harmonize PIPA with other jurisdictions to make it easier for businesses to operate in all jurisdictions?**

**2. Are there specific amendments to PIPA needed to modernize the Act for relevant businesses and organizations to conduct business in Alberta?**

[*] European Union, "Does the GDPR apply to Companies out of the EU?" available at https://gdpr.eu/companies-outside-of-europe/ (accessed February 7, 2024).
[†] There are exceptions for organizations with fewer than 250 employees. Small- and medium-sized enterprises (SMEs) are not exempt from the GDPR, but the regulation relieves them, in many cases, from record-keeping obligations. See Article 30.5 and European Union, "Does the GDPR apply to companies outside of the EU?" available at https://gdpr.eu/companies-outside-of-europe/ (accessed February 7, 2024).
[‡] Office of the Information and Privacy Commissioner for British Columbia, Guidance Document: Competitive Advantage Compliance with PIPA and the GDPR, March 2018, p. 3., https://www.oipc.bc.ca/guidance-documents/3923 (accessed February 7, 2024).
[§] European Union, "What is the GDPR, the EU's new data protection law?" available at https://gdpr.eu/what-is-gdpr/ (accessed February 7, 2024).

## 3.0 Artificial Intelligence

One of the most significant changes to the technological landscape is artificial intelligence (AI).[*] Artificial intelligence is a computer system that engages in machine learning, where computers analyze vast quantities of information, draw inferences, and make predictions from patterns within datasets.

In their joint-special report from 2021, Jay Chalke, Michael McEvoy, and Diane McLeod (respectively the Ombudsperson of British Columbia, the Information and Privacy Commissioner of British Columbia, and the then Ombudsman and Information and Privacy Commissioner of Yukon Territory, now the Information and Privacy Commissioner of Alberta) explain that increasing amounts of data – often derived from personal information – are required to develop, improve, achieve, and use artificial intelligence models.[†] Chalke et al. note that "we are generating data at an unprecedented speed."[‡]

The authors further explain that

> the risk of data that is collected, used, and retained for a particular purpose . . . being repurposed for something entirely different . . . without the consent of the data subject grows as AI-enabled tools become more capable and accessible.[§]

Chalke et al. describe situations in which automated decision systems (ADS) use personal information in ways that are either not authorized by individuals and/or that potentially cause harm to individuals.

One problem is that the input data itself may be inaccurate or biased and may require significant contextual information to be processed without causing harm to that individual. Bias in automated decision systems (ADS) can produce uneven outcomes for people, and a lack of algorithmic transparency makes it even more difficult to appeal an ADS decision in an informed manner.[**] Any request for algorithmic transparency, in turn, may be at odds with proprietorship. While some companies may look to governments to establish regulatory frameworks for the responsible use of AI, other companies may be reluctant to fulfill obligations associated with transparency and accountability because they are concerned about disclosing commercial proprietary information.

The challenge for governments is balancing support for an emerging and rapidly expanding AI sector while creating the conditions to foster public trust. Several legislative initiatives trying to establish that balance are currently under consideration.

The European Union Council and Parliament reached a provisional agreement for the *Artificial Intelligence Act* on December 9, 2023. Distinct from the GDPR, this Act is the first attempt at a comprehensive legal framework around AI. The Act[††]

- establishes obligations for AI based on its potential risk and level of impact

[*] *Artificial Intelligence and Data Act* defines an artificial intelligence system 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 to generate content or make decisions, recommendations or predictions" (s. 5).
[†] See Jay Chalke, Michael McEvoy, and Diane McLeod-McKay, Getting Ahead of the Curve: Meeting the Challenges to Privacy and Fairness Arising from Artificial Intelligence in the Public Sector, Joint Special Report No. 2, 2021, p. 21, available at https://www.oipc.bc.ca/special-reports/3546 (accessed on February 2
[‡] "There are 2.5 quintillion bytes of data created each day at our current pace, but that pace is only accelerating with the growth of the Internet of Things (IoT). Over the last two years alone 90 percent of the data in the world was generated." Chalke et al., p. 7; Cameron F. Kerry, Protecting Privacy in an AI-driven World, Brookings Institution, February 10, 2020, available at https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/ (accessed August 23, 2023).
[§] Chalke et al., p. 18.
[**] Chalke et al., p. 9.
[††] European Union, "Artificial Intelligence Act; deal on comprehensive rules for trustworthy AI," press release, December 9, 2023 https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

- bans applications that are a potential threat to citizens' rights and democracy[*]
- permits specific targeted uses of biometric identification systems for law enforcement purposes
- defines obligations for high-risk AI systems (that is, risks to health, safety, fundamental rights, environment, democracy and the rule of law)
- establishes guardrails for general AI systems (i.e., Chat GPT and other models)
- promotes measures for regulatory sandboxes and real-world testing of AI solutions without undue pressure from industry giants
- defines sanctions for non-compliance

In Canada, Quebec's QPSA is the only legislation currently enacted that imposes some obligations regarding ADS. However, it still needs to be determined if this legislation will effectively mitigate challenges with respect to the use of personal information from the latest developments in artificial intelligence.

Bill C-27 has some limited provisions related to ADS; it defines ADS and requires an organization to have information available in plain language that explains its use of any ADS and any potential impacts its use could have on an individual.[†]

The Office of the Privacy Commissioner of Canada (OPCC) examined AI as it relates to PIPEDA. The OPCC argued that "AI presents fundamental challenges to all PIPEDA principles" and conducted public consultations to identify several areas where the Act could be enhanced "for ensuring appropriate regulation of AI" and published the results in November 2020.[‡] Based on these consultations, the Office of the Privacy Commissioner of Canada made recommendations for PIPEDA reform.[§]

In the view of the OPCC, an appropriate law for AI would

- allow personal information to be used for responsible AI innovation and societal benefits
- authorize these uses within a rights-based framework
- entrench privacy as a human right and a necessary element for the exercise of other fundamental rights
- create provisions for automated decision-making to ensure transparency, accuracy and fairness; and
- require businesses to demonstrate accountability to the regulator upon request such as through enforcement measures, such as inspections, to ensure compliance with the law.[**]

The federal government has introduced the *Artificial Intelligence and Data Act* (AIDA) as part of Bill C-27.

AIDA states that its purposes are twofold:

- to “regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems” (s. 4(a)).

[*] The Act will include provisions that ban: biometric categorization that uses sensitive characteristics (i.e. certain beliefs, sexual orientation, race); untargeted scraping of facial images from the internet or CCTV to create facial recognition databases; emotion recognition in the workplace and educational institutions; social scoring based on social behaviour or personal characteristics; AI systems that manipulate human behaviour to circumvent their free will;
AI used to exploit people's vulnerabilities (due to age, disability, social or economic situation).
[†] There are ADS provisions in Bill C-27 in the *Consumer Privacy Protection Act*, see sections 2(1), 62(2)(c), 63(3).
[‡] Office of the Privacy Commissioner of Canada, “Consultation on artificial intelligence,” available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/ (accessed February 27, 2023).
[§] Ibid.
[**] Office of the Privacy Commissioner of Canada, "A Regulatory Framework for AI: Recommendations for PIPEDA Reform," available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/ (accessed February 27, 2023).

- to “prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests” (s. 4(b)).[*]

Under AIDA, responsible persons must identify, assess, and mitigate risks of harm when operating high-impact AI systems (s. 8). The same persons are required to notify the Minister if a system for which they are responsible results in, or is likely to result in, material harm (s. 12). The Act also creates the role of the Artificial Intelligence and Data Commissioner, that is a senior official in the department, not an independent Commissioner (s. 33(1)). The legislation also permits the application of administrative monetary penalties (not fines) to persons who have violated the Act and permits the treatment of a breach of the Act as an offence (ss. 29-30). Despite these details, the regulations rather than the legislation will determine crucial provisions of AIDA.

Notably, AIDA focuses on international and interprovincial trade and commerce (the federal jurisdiction). Consequently, provinces have the latitude to enact legislation mitigating risks to individual privacy from artificial intelligence provincially.

Alberta’s PIPA is drafted to use technologically neutral language, meaning that the legislation does not refer to specific types of records or technology. The advantage of this strategy is that it has been possible to apply the provisions of PIPA to personal information that is collected, used, and disclosed electronically.[†] Going forward, a primary concern may be how technology is rapidly changing and the vast amounts of personal information used to facilitate these changes.

**Question**

**Should PIPA include a framework to regulate the design, development, and/or use of artificial intelligence systems within Alberta? If so, what should be included?**

[*] “Harm” means “physical or psychological harm to an individual; damage to an individual’s property; or economic loss to an individual” (s. 5).

[†] As discussed in the section on "consent requirements" in this document, Alberta's PIPA – like all comparable legislation in Canada - establishes consent as the primary mechanism individuals may use to control the collection, use, and disclosure of their personal information by organizations. In the current circumstances of rapid technological change, it is increasingly difficult for individuals to provide meaningful consent to how their electronic information is used.

## 4.0 Application

PIPA applies to all organizations concerning all personal information (s. 4(1)). An organization is defined in section 1(1)(i) as:

- a corporation,
- an unincorporated association,
- a trade union as defined in the *Labour Relations Code,*
- a partnership as defined in the *Partnership Act*, or
- an individual acting in a commercial capacity.

PIPA does not apply to individuals collecting, using, and/or disclosing personal information only for personal or domestic purposes.

### 4.1 Non-profit Organizations

Under PIPA, there are special provisions for certain non-profit organizations that are incorporated under the *Societies Act* or the *Agricultural Societies Act*; are registered under Part 9 of the *Companies Act*; or meet the criteria established under the regulations to qualify as a non-profit organization (s. 56(1)(b)).

These non-profit organizations are not required to follow the rules in the Act when collecting, using, or disclosing personal information except when they engage in a commercial activity(s. 56(2)). "Commercial activity" means any transaction, act, or conduct or any regular course of conduct that is of a commercial character (s. 56(1)(a)). This includes:

- selling, bartering, or leasing membership, donor, or other fundraising lists
- the operation of a private school or early childhood services program as defined in the *School Act*; and
- the operation of a private college as defined in the *Post-secondary Learning Act* (s. 56(1)(a)).

Other organizations may operate on a not-for-profit basis. However, organizations that do not meet the definition of a non-profit organization under section 56 of PIPA must fully comply with the entire Act for handling the personal information of their clients, employees, volunteers, and donors, regardless of whether they are carrying out a commercial activity.

The *Consumer Privacy Protection Act* (CPPA) portion of Bill C-27 includes similar proposals to those already present in PIPEDA and in Alberta's PIPA: charities and non-profit organizations are subject to the Act when they engage in commercial activities (s .2(1) and 6(1)).

In contrast, the GDPR applies to processing personal information by all organizations (including non-profit organizations) regardless of whether the processing occurs during commercial activities (recitals 1-4).

Quebec's QPSA applies to organizations engaging in economic activities even if that activity is not commercial in nature. However, the organization's primary purpose is an essential factor in QPSA's applicability.

BC PIPA applies to all private-sector organizations, including non-profit organizations.

### 4.2 Political Parties

Political parties are not defined as organizations under Alberta's PIPA. Alberta PIPA has specific exemptions for registered constituency associations, provincial registered parties and individuals running for office (ss. 4(3)(m) and (n)). In contrast, British Columbia's PIPA has been found to apply to both

provincial and federal political parties operating in BC.[*] Similarly, Quebec's QPSA applies to personal information held by a political party, an independent Member, or an independent candidate (s. 1).

**Questions:**

**1. Should all non-profit organizations be fully subject to PIPA for all their activities?**

**2. Should PIPA apply to political parties?**

[*] Office of the Information and Privacy Commissioner for British Columbia, Investigation Report P19-01 Full Disclosure: Political parties, campaign data, and voter consent, February 6, 2019, available at https://www.oipc.bc.ca/investigation-reports/2278 (accessed September 13, 2022); and Guidance Document: Political Campaign Activity, August 2022, available at https://www.oipc.bc.ca/guidance-documents/3700 (accessed September 13, 2022).

## 5.0 Protections of Sensitive Personal Information

PIPA provides rules for the collection, use, and disclosure of personal information. The stated purpose of PIPA is

> to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have their personal information protected and the need of organizations to collect, use or disclose personal information in a way that is reasonable (s. 3).*

Personal information is information that is about an identifiable individual (s. 1(1)(k)).

### 5.1 Sensitive Personal Information

Some legislation sets out specific provisions for certain categories of personal information, such as sensitive personal information, children's personal information, and biometrics.

The GDPR sets out particular categories of personal data for sensitive personal information, such as data, that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, sexual orientation, genetic data or biometric data. This information is subject to additional protections (Article 9).

Quebec's QPSA also sets out additional protections for sensitive personal information that "due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, it entails a high level of reasonable expectation of privacy" (s. 12). The Act additionally includes protections for personal information collected using technology that has functions allowing the person concerned to be "identified, located, or profiled" (s. 8.1).†

#### 5.1.a Biometric Information

Some examples of biometric data collected in the private sector are facial images, iris scans, voice recognition applications, fingerprint access systems, keystroke monitoring, and geolocation.‡

Under PIPA, biometric information is considered personal information, and it is therefore subject to the Act's general rules for collection, use, disclosure, and protection.

The GDPR defines biometric data as

> personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data (Article 4(14)).

---

* PIPA defines reasonable as what a reasonable person would consider appropriate in a given circumstance (s. 2).

† Profiling is "the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behaviours" (s. 8.1).

‡ For examples of how this information has been used in ways that violate Canadian privacy laws, please see Office of the Information Privacy Commissioner of Alberta, News Release: Tim Hortons app violated privacy laws in collection of 'vast amounts' of sensitive location data, June 1, 2022, available at https://oipc.ab.ca/p2022-ir-01/ (accessed September 6, 2022); and News Release: Clearview AI's Unlawful Practices Represented Mass Surveillance of Canadians, Commissioners Say, February 3, 2021 available at https://oipc.ab.ca/p2021-ir-01/ (accessed September 6, 2022).

In Quebec, sensitive personal information includes medical and biometric information (see s. 12), and individuals must expressly consent to the use of this information (ss. 12 and 14).

### 5.1.b Children's Personal Information

PIPA's current provisions apply to children's personal information in the same ways as to the personal information of adults. The legislation recognizes mature minors as being capable of exercising their rights and powers defined by PIPA if they understand the nature of the right or power and the consequences of exercising that right or power (s. 61(1)(c)).

Other jurisdictions have included specific provisions to protect children's personal information. Under the GDPR, for example, processing the personal data of any child under 16 requires parental consent, and the data itself may be subject to special protections (Article 8 and Recital 38).

Quebec's QPSA also sets out specific protections for children's personal information. The Act requires that the use of the personal information of a minor under 14 years of age be "given by the person having parental authority or by the tutor."[*] For children over 14 years of age, the child, the person with parental authority or the tutor may grant consent (s. 14).

At the federal level, proposals in the CPPA include provisions concerning minors' personal information. Personal information of minors is considered sensitive information, and parents, guardians, and tutors are authorized to exercise the rights and recourse under the Bill on behalf of their child, including consent (ss. 2(2), 2(4)(a)). If the child is capable, the child may object to their parents' authorization (s. 2(4)(a)). Minors are also granted more expansive rights than adults to have their personal information deleted, whereby exceptions apply to requests for the erasure of the personal information of adults but not for the personal information of minors (ss. 55(2)(d) and (f)).

**Questions:**

**Should provisions be added to PIPA to further protect potentially sensitive information? If so, for which information?**

**Should provisions be added for biometric information?**

**Should provisions be added to enhance the protection of children's personal information?**

[*] In Quebec law, a tutor is an appointed individual responsible for the represented person's well-being. Government of Quebec. "Tutorship to a person of full age," https://www.quebec.ca/en/justice-and-civil-status/legal-protection/tutorship-person-full-age

## 6.0 Consent Requirements

Although consent is a cornerstone of Canadian privacy law, commentators have noted that obtaining meaningful consent is increasingly challenging as technology changes. Privacy expert Dr. Teresa Scassa describes the potential problems associated with obtaining meaningful consent as follows:

> On the one hand, consent is an important means by which individuals can exercise control over their personal information; on the other hand, it is widely recognized that the consent burden has become far too high for individuals who are confronted with long, complex and often impenetrable privacy policies at every turn. At the same time, organizations that see new and emerging uses for already-collected data seek to be relieved of the burden of obtaining fresh consents. The challenge in privacy law reform has therefore been to make consent meaningful, while at the same time reducing the consent burden and enabling greater use of data by private and public sector entities.[*]

PIPA establishes consent as the primary mechanism individuals may use to control organizations' collection, use, and disclosure of their personal information. Except in circumstances specified by PIPA, an organization must obtain consent to collect, indirectly collect, use, and disclose personal information about an individual (s. 7). The Act allows for three types of consent:

- **express consent** – consent given verbally or in writing, including via electronic communications (ss. 8(1) and (5))
- **implied or deemed consent** – consent given voluntarily for a purpose that is reasonable and well understood (ss. 8(2), (2.1) and (2.2));
- **consent by not opting out** – consent deemed to have been granted if a reasonable opportunity to decline or object was provided but not acted upon (s. 8(3)).

Under PIPA, an organization may collect personal information without consent if it is of a type and amount that is reasonable and only for reasonable purposes (ss. 11(1) and (2)). Before or at the time of collecting personal information from the individual, the organization must give notice to the individual explaining the purposes for collection and the name of a person who can answer questions about the collection (s. 13(1)).

### 6.1 Plain Language

Under the GDPR, consent is obtained through any "freely given, specific, informed, and unambiguous indication of the data subject's wishes by a statement or clear affirmative action" (Article 4(11)). Consent must be sought using language that is intelligible and easily accessible and controllers[†] must provide information notices to ensure transparency of processing. Visualization through standardized icons is encouraged, and messaging should be clear and in plain language (Article 7).

Quebec's QPSA provides that "consent under this Act must be clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language" (s. 14). CPPA provides for express consent and implied consent. Under the proposals in CPPA, consent must be obtained in plain language (s. 15).

[*] Teresa Scassa, "Bill C-27's Take on Consent: A Mixed Review," available at https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=355:bill-c-27%E2%80%99s-take-on-consent-a-mixed-review&Itemid=80 (accessed February 7, 2024).

[†] The GDPR defines any entity that collects, uses, or discloses personal information of EU residents as a "controller" or a "processor."

**Questions:**

**1. Are the provisions in PIPA dealing with forms of consent and the conditions attached to their use appropriate?**

**2. Should individuals receive notice in plain language when organizations explain the purposes for which personal information is collected, used or disclosed?**

## 7.0 Individual Rights that are Not Included Under PIPA

### 7.1 Right to Erasure

Under PIPA, an individual may withdraw or vary consent by giving the organization reasonable notice (s. 9(1)) if this withdrawal or variance does not prevent the individual or organization from meeting a legal obligation (s. 9(5)). An organization may retain personal information only for as long as the organization reasonably requires the information for a legal or business purpose. After such a time, the information must be destroyed or anonymized. Notably, PIPA has no provisions whereby an individual may require an organization to erase, dispose or de-index the personal information it holds about that individual.

The GDPR includes the right to erasure, including de-indexing from an online search, with certain limitations and exceptions (Article 17).* The right to be forgotten and the right to erasure are sometimes treated interchangeably.

Quebec's QPSA includes provisions for de-indexing that came into force on September 22, 2023. Section 28.1 of the QPSA states:

> The person to whom personal information relates may require any person carrying on an enterprise to cease disseminating that information or to de-index any hyperlink attached to his name that provides access to the information by a technological means, if the dissemination of the information contravenes the law or a court order.

The CPPA does not mention de-indexing. Subject to certain exceptions, CPPA requires that an organization dispose of an individual's personal information as soon as feasible. The CPPA grants minors more expansive rights than adults for deleting personal information: must comply with requests to delete the information of minors, whereas there are instances where organizations may refuse the request about the personal information of adults (see ss. 55(2)(d) and (f)).

### 7.2 Right to Data Portability

Under the GDPR, individuals can obtain a copy of their personal data from a controller. The controller must provide the copy in a structured, commonly used, machine-readable format. The individual may request that the data be transmitted to another controller, allowing individuals to obtain, transfer, and reuse their personal (electronic) data for their own purposes (Article 20).

CPPA provides for data portability only if a "data mobility framework" exists between organizations. Organizations subject to a data mobility framework must disclose the personal information of a requesting individual to the other organization (s. 72). The CPPA does not define data mobility frameworks and leaves this subject to future regulation (s. 123).†

### 7.3 Right to Information about the Logic Involved in Automated Decision Systems (ADS)

The concept of algorithmic transparency includes providing clear information about the logic involved in ADS.

Under the GDPR, individuals who are subject to an ADS have a right to meaningful information about the logic involved. This information may include the factors considered in the decision and how those factors are weighted. Individuals also have a right to be notified about being subject to fully automated decision-making systems and to know the significance and potential consequences of such processing. A person

* Article 17(3) defines exceptions for deletion requests: adverse effects to the freedom of expression, contradiction of a legal obligation, acts against the public interest in the area of public health, acts against the public interest in the area of scientific or historical research, or if it prohibits the establishment of a legal defence or exercise of other legal claims.

† These regulations must prescribe "parameters for the technical means for ensuring interoperability in respect of the disclosure and collection" of personal information subject to the data mobility framework (s. 123).

may also opt out of being subject to automated decision-making with a legal or similarly significant effect (Articles 13, 14, 22).

Quebec's QPSA requires that any organization that exclusively uses "automated processing" to render a decision about an individual must be informed of:

- the personal information used to render the decision
- the reasons and the principal factors and parameters that led to the decision
- the right of the person concerned to have the personal information used to render the decision corrected
- the person concerned must be given the opportunity to submit observations to the employee of the organization designated to review the decision (s. 12.1).

The CPPA defines ADS as

> any 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 (s. 2(1)).

The CPPA would require an organization using ADS to provide a general account of the ADS and, on request by an affected individual, give the individual with an explanation of the prediction, recommendation or decision in plain language (ss. 62(2)(c), 63).

**Questions:**

**1. Should PIPA include other protections for individual information, such as an individual's right to be forgotten or de-indexed?**

**2. Upon an individual's request, should organizations be required to transfer that individual's digital personal information to another organization in a structured, commonly used, and machine-readable format when it is technically feasible (data portability)?**

**3. Should organizations be required to provide individuals with the logic involved in automated decision making about that individual (algorithmic transparency)?**

## 8.0 Safeguarding Personal Information

### 8.1 De-identification of Personal Information

Legislation provides for using and processing personal information, including when information may be anonymized or de-identified. De-identified information is not the same as anonymized information. Anonymized data is the process of irreversibly and permanently transforming personal data, making it impossible to determine the individual's identity. Organizations that anonymize data tend to do so for specific purposes because anonymizing data is a more technical process.[*]

Under PIPA, an organization must make reasonable security arrangements to safeguard against unauthorized access, collection, use, disclosure, duplication, modification, disposal, or destruction of personal information that is in the organization's custody or under its control (s. 34). An organization may only retain personal information for as long as it reasonably needs for legal or business purpose (s. 35(1)). When an organization no longer requires personal information for legal or business purposes, it must destroy or "render the personal information non-identifying." According to the Act, non-identifying information "can no longer be used to identify an individual" (ss. 35(2)(a) and (b)).

QPSA defines personal information as de-identified if it no longer allows the person concerned to be directly identified (s. 12). The Act permits the use of de-identified personal information without the consent of the person concerned for the specific purposes of research or the production of statistics (among other reasons specified in the legislation) (s. 12). However, those using de-identified information must take reasonable measures to limit the risk of identifying a person whose information was de-identified (s. 12). QPSA requires the destruction or anonymization of personal information when an organization has achieved its purposes for collecting or using personal information (s. 23). Anonymization processes should be done following generally accepted best practices and in accordance with criteria defined in regulation (s. 23).

The CPPA defines the term "de-identify" as modifying an individual's personal information so that they cannot be directly identified. However, should a dataset be reassembled, there is still a risk of identification (s. 2(1)). The CPPA proposes that organizations may use de-identified information for specific purposes, including internal research, analysis, and development.

The GDPR provides rules for processing "pseudonymized data" but not anonymized data since the latter cannot be identified and is, presumably, not a risk to an individual's privacy. Pseudonymized data under the GDPR is similar to de-identified data under the CPPA. The GDPR defines pseudonymization in Article 4(5) as

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject (individual person *who* can be identified) without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[*] For a helpful website explaining the difference between pseudonymization, anonymization and encryption, please see Statice, "Pseudonymization vs. anonymization: differences under the GDPR," available at https://www.statice.ai/post/pseudonymization-vs-anonymization#:~:text=Pseudonymization%20holds%20a%20higher%20likelihood,while%20anonymized%20data%20isn%27t (accessed September 7, 2022).

### 8.2 Privacy Management Program

A privacy management program ensures that privacy is built into all initiatives, programs, or services for the responsible management of personal information.[*]

Alberta's PIPA has elements of a privacy management program in the Act (ss. 5(3), 6). An organization must designate an individual to oversee and ensure compliance with the Act. The organization must develop and follow reasonable policies and practices that meet its obligations under the Act and provide them in writing upon request.

The GDPR provides for privacy by design and default: an organization must "implement appropriate technical and organisational measures" to protect personal information. The GDPR acknowledges reasonable parameters for this measure by balancing the "cost of implementation and the nature, scope, context and purposes of processing as well as the risks" to the individual involved (Article 25).

Under the provisions of QPSA, every organization must establish and implement personal information protection policies and practices. The policies and practices must include a framework that defines the management and destruction of information, the roles and responsibilities of the organization's personnel when managing personal information, and a process for dealing with complaints about personal information management and use. All of this information should be published on the organization's website or in another appropriate medium in simple and clear language (s. 3.2).

Under CPPA, every organization must implement and maintain a privacy management program that includes the policies, practices, and procedures to fulfill its obligations under the Act. At the Commissioner's request, an organization must provide access to its privacy management program and the Commissioner may provide guidance on or recommend corrective measures (see ss. 9 and 10).

### 8.3 Privacy Impact Assessment

A privacy impact assessment is a process used to identify, assess and mitigate privacy risks to an individual. This assessment could be required if

- an organization uses a service provider and there is information sharing outside the organization;
- the organization uses automated processes or artificial intelligence in the processing of personal information;
- personal information is being de-identified, re-identified, or anonymized;
- biometric information (for example, facial recognition) or geolocation information is collected, used, or disclosed.

Under the GDPR, an organization must carry out a privacy impact assessment if the processing an individual's data is likely to result in a high risk to the rights and freedoms of individuals (Article 35). The assessment must be complete and documented before starting the intended data processing.

The CPPA portion of Canada's Bill C-27 proposes using a privacy impact assessment when an exemption to consent may occur. An organization may collect or use an individual's personal information without their knowledge or consent in certain circumstances. Consent is needed if an organization has a "legitimate interest" in the collection or use of personal information that outweighs any potential adverse effect on an individual. CPPA stipulates that this is permitted if

- the individual would expect the collection and use, and

[*] Office of the Information and Privacy Commissioner for British Columbia, Guidance Document: Competitive Advantage Compliance with PIPA and the GDPR, March 2018, p. 18, available at \\zeus.Lao.local\shared$\COMMON\LIBRARYHS\Research\Committees\LPCs\AB's Economic Future\PIPA\PIPA 2022\Reviews and Reports\BC_PIPAReview_2020-21\GD GDPR vs PIPA March 2018.pdf (accessed September 27, 2022).

- it is not to influence the behaviours or decisions of those individuals.

To be exempt from obtaining consent in this situation, an organization must identify any potential adverse effects on the individual that are likely to result from the collection of the information, take reasonable measures to reduce those risks and document how the organization's collection or use of the personal information complied with any prescribed requirements (s. 18).

**Questions:**

**1. Should PIPA regulate the de-identification and/or anonymization of personal information within the control of an organization and the subsequent use or disclosure of the de-identified or anonymized information? If so, how?**

**2. Should organizations be required to have a privacy management program and provide written information about the program to individuals and the Commissioner?**

**3. Should organizations be required to complete and submit a privacy impact assessment to the Commissioner for specific initiatives involving personal information?**

## 9.0 Breach Notification

Privacy breaches can have significant consequences for individuals, ranging from identity theft and fraud to financial loss, humiliation, and anxiety.

PIPA requires an organization that suffers a loss or unauthorized access to or disclosure of personal information (breach) to notify the Office of the Information and Privacy Commissioner (OPIC) without an unreasonable delay if the breach poses a real risk of significant harm to affected individuals (s. 34.1(1), Regulation, s. 19). If the Commissioner determines that the breach poses a real risk of significant harm, the Commissioner may then require the organization to notify individuals affected by the breach and to do so within a specified period (s. 37.1(1)). The Act's provisions do not restrict an organization's ability to notify individuals on its own initiative, before or after informing the Commissioner, even if the incident does not give rise to a real risk of significant harm (s. 37.1(7)).[*]

OIPC reviews all breach reports and issues a decision on them. Between 2010 and 2021, the OIPC issued 1,953 decisions. Of these, 1,334 were decisions involving a real risk of significant harm, representing 68 per cent of all decisions. Between 2017-2018 and 2020-2021, 70 to 80 per cent of decisions involved a real risk of significant harm. Further, the number of reported breaches is increasing each year, which may suggest that more breaches are occurring overall.[†]

When a breach occurs under GDPR, the processor must notify the Commissioner in each country within 72 hours (Article 33) and affected individuals must be notified without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of the individual (Article 34).

Under Quebec's QSPA, when a breach is determined to present a risk of serious injury, the organization must promptly notify the Commission d'accès à l'information and any person whose personal information is affected by the incident (s. 3.5). In assessing the risk of injury, the organization must consider the sensitivity of the breached information, the anticipated consequences of that information's use, and the likelihood that the information will be used for injurious purposes (s. 3.7).

Under the CPPA, notification of the Commissioner and impacted individuals is required "as soon as feasible" if it is reasonable to believe that the break creates a real risk of significant harm to the individual (ss. 58(1-8)).

**Question:**

**Are the provisions for notification of breaches to the Commissioner and individuals under PIPA appropriate?**

[*] If an organization notifies individuals in a way that does not meet the requirements of the Act and Regulation, the Commissioner may require the organization to provide further notification.

[†] The OPIC notes that there "were 377 breach reports submitted to the OIPC in 2020-2021, compared with 50 in 2010-2011. This suggests more organizations recognize the importance of responding to privacy breaches and are aware of the requirement to report certain breaches to the OIPC and to notify affected individuals." Office of the Information and Privacy Commissioner of Alberta, PIPA Breach Report 2022, p. 2, available at https://oipc.ab.ca/wp-content/uploads/2022/07/PIPA-Breach-Report-2022.pdf (accessed September 15, 2022).

## 10.0 Administrative Monetary Penalties

Administrative monetary penalties (AMP) are financial penalties imposed for the contravention of a regulatory scheme, not judicial fines. Under PIPA, there are penal provisions but no administrative monetary penalties.[*] Other jurisdictions have included administrative monetary penalties in their laws to address serious, repetitive, or long-term contraventions and to reinforce that individuals' privacy rights are protected and enforced. Administrative monetary penalties may be imposed under the GDPR, the proposals in Bill C-67 and Quebec's QPSA.

According to the GDPR, administrative monetary penalties should be "effective, proportionate, and dissuasive" (Article 83(1)). The maximum fine for certain infringements is the greater of €20 million or up to four per cent of the total worldwide annual turnover[†] of the preceding financial year (Article 83(5)). The maximum fine for lesser infringements is the greater of €10 million or up to two per cent of the total worldwide annual turnover of the preceding financial year (s. 83(4)).

Quebec's QPSA provides for the Commission d'accès à l'information to impose monetary administrative penalties and sets out the terms for recovering and claiming the amounts owing. Administrative monetary penalties of up to $50,000 may be imposed if the contravener is an individual. In the case of an organization the greater of $10 million or two per cent of worldwide turnover for the preceding fiscal year, may be levied (see s. 90.12).

At the federal level, the CPPA proposes that the regime for administrative monetary penalties be established by regulation (s. 29(4)) and that the purpose of the proposed administrative monetary penalties "is to promote compliance . . . and not to punish" (ss. 29(2) and 95(6)). Under the proposals in CPPA, the Personal Information and Data Protection Tribunal may impose a maximum penalty of the higher of $10,000,000 or three per cent of the organization's annual gross global revenue for a limited list of infractions (s. 95(4)).

**Question:**

**Should PIPA include the ability of the Commissioner to levy administrative monetary penalties against an organization for certain contraventions of the Act?**

[*] The penal provisions in Alberta's PIPA are as follows: if the Commissioner thinks that an organization or individual has committed an offence, the Commissioner may refer the matter to the Crown for prosecution. A person who commits an offence under the Act is liable to a fine of up to $10,000 in the case of an individual and up to $100,000 in the case of an organization (s. 59(2)). The Commissioner does not have authority to apply penalties or levy fines. An Alberta Provincial court judge assesses fines following a conviction. Section 59(1) of PIPA defines when an offence is committed under the Act.

[†] Total worldwide turnover is equivalent to total annual revenue.

## Appendix A – Jurisdictional Summary Tables of Emerging Issues

**Table 1 Application of Selected Privacy Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Whenever personal data of individuals located in the EU is processed | To federal works, undertakings, and businesses that are within the jurisdiction of parliament; and to organizations, including an association, a partnership, a person or a trade union, in respect of personal information that the organization collects, uses or discloses in the course of commercial activities. | To organizations based and operating in Quebec.<br><br>The Act also applies to personal information held by a political party, an independent Member or an independent candidate to the extent provided for by the *Election Act*. | To organizations that collect, use, or disclose personal information in Alberta, meaning:<br>• a corporation,<br>• an unincorporated association,<br>• a trade union<br>• a partnership<br>• an individual acting in a commercial capacity,<br>• and certain non-profit organizations when acting in a commercial capacity. |

**Table 2 Scope of Selected Privacy Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Whenever personal data is processed.<br>"Processing" is a broad term that covers almost anything that can be done with data, whether or not by automated means, including collection, storage, transmission, and analysis, etc. | Whenever personal data is collected, used, or disclosed | Whenever personal information is collected, held, used or communicated to third persons in the course of carrying on an enterprise.[*] | Whenever personal information is collected, used, or disclosed |

[*] The definition of "enterprise" is set out in s. 1525 of the *Civil Code of Québec*, CQLR c. CCQ 1991 as "[t]he carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service."

**Table 3 Definition of Personal Information in Selected Privacy Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Information relating to identified or identifiable person | Information about an identifiable individual<br>Includes provisions with respect to personal employee information of any federal works, undertakings, and businesses that are within the jurisdiction of the Parliament of Canada. | Personal information "is any information which relates to a natural person and directly or indirectly allows that person to be identified." | Information about an identifiable individual<br>Includes provisions with respect to personal employee information in Alberta organizations. |

**Table 4 Provisions for Sensitive Personal Information in Selected Privacy Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| The GDPR sets out additional protections for "special personal data" relating to sensitive personal information: data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; and data concerning health or sex life and sexual orientation; genetic data or biometric data.<br>Children have specific protections for their personal data. | Personal information of minors is considered "sensitive information" and children have specific protections for their personal data. | Sets out additional protections for "sensitive personal information" defined as information that "due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, entails a high level of reasonable expectation of privacy."<br>Includes protections for personal information collected using technology that allows the person concerned to be "identified, located, or profiled."<br>Minors under 14 years of age have specific protections for their personal information. | None. |

**Table 5 Forms of Consent Provided for in Selected Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Consent means any "freely given, specific, informed, and unambiguous indication of the data subject's wishes by a statement or clear affirmative action" agreeing to the processing of their personal data.<br><br>Explicit consent is required for processing special categories of data; for automated individual decision making, including profiling; and for international data transfers. | Permits:<br><br>• express consent and<br>• implied consent.<br><br>This is measured on a level of reasonableness and considers the sensitivity of the information.<br><br>Consent must be obtained in plain language. | Permits:<br><br>• Express consent that "must be clear, free and informed and be given for specific purposes."<br><br>Express consent is required for "sensitive personal information."<br><br>Consent must be obtained in "clear and simple language." | Permits:<br><br>• express consent,<br>• deemed consent, and<br>• opt-out consent (when consent is presumed, but an individual can decline).<br><br>Consent is measured on a level of reasonableness. |

**Table 6 Rights Defined in Selected Privacy Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| The GDPR is rights-based legislation and directly prescribes the following:<br><br>• Right to be informed<br>• Right to access<br>• Right to correction of personal information<br>• Right to erasure<br>• Right to restriction of processing<br>• Right to data portability<br>• Right to object to data processing activities<br><br>Right to logic behind automated decision systems | The preamble to Bill C-27 refers to rights. In addition, the provisions of the CPPA appear to provide for an individual's:<br><br>• Right to be informed<br>• Right to access<br>• Right to request correction of personal information<br>• Right to disposal of personal information<br>• Right to data portability if a data mobility framework is in place between organizations<br>• Right to logic behind automated decision making<br><br>Individuals have the right to withdraw or change consent. | • Right to be informed<br>• Right to access<br>• Right to request correction of personal information<br>• Right to erasure<br>• Right to logic behind automated decision systems<br><br>Individuals have the right to withdraw consent. | Alberta's PIPA establishes consent as the primary mechanism by which individuals may use to control the collection, use and disclosure of their personal information by organizations. The provisions of PIPA do not refer to rights. Nevertheless, PIPA provides an individual's:<br><br>• Right to be informed<br>• Right to access personal information<br>• Right to request correction of personal information<br>• Right to request information about the use and disclosure of personal information<br><br>Individuals have the right to withdraw or change consent. |

**Table 7 Anonymization and De-identification of Personal information in Selected Privacy Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Provides rules for the use of "pseudonymized data" – that is personal information processed in such a manner that the personal data can no longer be used to identify an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that identification is impossible. | Personal information may be used without consent if the information is de-identified for internal research, analysis, and development. | Personal information may be used without the consent of the person concerned for the specific purposes of research or for the production of statistics and if the information is de-identified. | No provision. |

**Table 8 Provisions for Privacy Management Programs in Selected Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| The GDPR provides for privacy by design and by default. Organizations must "implement appropriate technical and organisational measures" to protect personal information that take into account "cost of implementation and the nature, scope, context and purposes of processing as well as the risks" to the individual involved. | Every organization must implement and maintain a privacy management program that includes the policies, practices, and procedures the organization has in place to fulfill its obligations under the Act. On the request of the Commissioner, the organization must provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program and provide guidance on or recommend that corrective measures to its privacy management program. | Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information. Such policies and practices must provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information.<br><br>• The policies and practices must be published in clear language on the organization's website. | An organization must designate individual(s) to provide oversight for PIPA compliance and develop and follow policies and practices that are compliant. The organization must provide written information about those policies and practices upon request. Policies and practices must include information on collection, use and disclosure and the purposes for which a service outside of Canada is used, if relevant. |

**Table 9 Provisions for Privacy Impact Assessments in Selected Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Mandatory before initiating any processing that may have a high risk of infringing on individual rights | Organizations relying on the legitimate interest exception will be required to complete a privacy impact assessment and to provide copies of the assessment to the Commissioner on request. | Mandatory "for any project to acquire, develop or overhaul an information system or electronic service delivery system" involving personal information." | |

**Table 10 Provisions for Breach Notifications in Selected Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Notification required within 72 hours to the Commissioner in each country (called the "supervisory authority"), and to individuals "without undue delay" when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. | Notification required as soon as it is feasible to the Commissioner and to the individual if it is reasonable to believe that the breach creates a real risk of significant harm to the individual. | The Commission d'accès à l'information and the affected individual must be notified promptly if the incident presents a risk of serious injury. | Notification is required to the Commissioner without unreasonable delay if the breach poses a real risk of significant harm to the individual. The Commissioner may then require the organization to notify individuals affected by the breach and to do so within a specified period of time. |

**Table 11 Provisions for Administrative Monetary Penalties in Selected Legislation**

| GDPR | CPPA | QPSA | AB PIPA |
|---|---|---|---|
| Serious infringement: up to 20 million Euros or four per cent of annual worldwide turnover. Lesser infringement: up to 10 million Euros or two per cent of annual worldwide turnover. | Maximum penalty of the higher of $10 million or three per cent of the organization's annual gross global revenue. | Maximum penalty of $50,000 in the case of a natural person and, in all other cases $10 million or, if greater, the amount corresponding to two per cent of worldwide turnover for the preceding fiscal year. | None. |

Sources: Office of the Information and Privacy Commissioner for British Columbia, Guidance Document: Competitive Advantage Compliance with PIPA and the GDPR, March 2018, p. 2, available at \\zeus.lao.local\shared$\COMMON\LIBRARYHS\Research\Committees\LPCs\AB's Economic Future\PIPA\PIPA 2022\Reviews and Reports\BC_PIPAReview_2020-21\GD GDPR vs PIPA March 2018.pdf (accessed August 25, 2022); House of Commons of Canada, Bill C-27, available at https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading (accessed September 15, 2022); Alberta, *Personal Information Protection Act*, S.A. 2003, c. P-6.5; Quebec, *Loi sur la protection des renseignements personnels dans le secteur privé/Act respecting the protection of personal information in the private sector*, CQLR c. P.39-1.