Alert

July 23, 2023

COZEN O'CONNOR

A Guide to Canada's New Proposed Privacy Law

Bill C-27, the Digital Charter Implementation Act, proposes new legislation that will significantly impact the Canadian privacy law landscape. The omnibus bill – which is a second reiteration of the former Bill C-11 (which failed to pass) – seeks to amend the Personal Information Protection and Electronic Documents Act (PIPEDA), among other acts, as well as introduce the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (PIDPTA), and the Artificial Intelligence and Data Act.

The proposed bill, and specifically the CPPA and PIDPTA, aims to align existing federal privacy laws with global standards by implementing significant changes. This article summarizes the bill's proposed changes to Canada's privacy laws (including notable new powers and penalties) and outlines best practices that businesses can adopt to ensure compliance with these new laws.

Canada's EU-inspired Bill

At a 30,000-foot view, the bill introduces more strenuous privacy laws akin to the European Union's General Data Protection Regulation (the GDPR), significant multi-million dollar penalties, and will substantially impact how businesses operating in Canada (or targeting Canadian consumers) handle and manage data.

The bill also proposes establishing a new tribunal, the Personal Information and Data Protection Tribunal, which will play a role in enforcing the CPPA. In particular, the tribunal will have the power to review the Privacy Commissioner of Canada's (the Privacy Commissioner) recommendations to impose administrative monetary penalties for certain contraventions of the CPPA and hear appeals from the Privacy Commissioner's decisions.

On April 24, 2023, the bill passed the second reading in the House of Commons and has now been referred to the Standing Committee on Industry and Technology for further consideration and consultation.

Application of the CPPA

Like PIPEDA, the CPPA will apply to all organizations that collect, use, or disclose personal information during commercial activities. This includes personal information collected, used, or disclosed across provincial or international borders.

The CPPA will also extend to employee information of federally-regulated organizations such as airlines and banks, but not to employee information held by other private sector organizations.

In line with PIPEDA, the CPPA will not apply to anonymized personal information.

Notable New Rules

Classification of Non-Personal Information

The CPPA establishes two categories of non-personal information:

- **Anonymous information** pertains to personal information that has been altered to eliminate the possibility of identifying individuals.
- **De-identified information** refers to personal information where the identifying elements have been removed, but there is still a risk of identification.

Anonymous information may be utilized and shared without restriction, whereas de-identified information will be subject to some regulation.

Any Obando Ospina

Associate

aobandoospina@cozen.com
Phone: (416) 639-6698
Fax: (416) 361-1405

Related Practice Areas

- Business
- Corporate
- Technology, Privacy & Data Security

New Consent Exemptions

The CPPA reinforces the scope around obtaining valid and informed consent for the collection, use, and disclosure of personal data while introducing several exemptions to consent, including:

- **Business Activities Exemption:** Businesses will be able to collect personal data without consent in certain situations, including the provision of a requested product or service, information, system or network security, and the safety of a product or service. Consent will also not be required where a reasonable person would expect the collection or use of the information. However, marketing purposes are not included under this exception.
- **Service Provider Exemption:** Organizations will be allowed to transfer personal data to their service providers without obtaining explicit consent. However, organizations will still be accountable to ensure that the service providers' management of that personal data complies with the CPPA.
- **Legitimate Interest Exemption:** Organizations will be able to collect, use, and disclose personal information without consent in circumstances where the organization's "legitimate interests" – a term that the CPPA does not further define – outweigh the adverse interests to the individual. The exemption does not apply if the personal information is to be "collected or used for the purpose of influencing the individual's behavior or decisions." To make use of this exemption, an organization must identify any potential adverse effects on the affected individual and take reasonable steps to mitigate or eliminate those effects. The organization must also keep a record of its assessment.
- **Socially Beneficial Purposes:** An organization may disclose an individual's *de-identified* personal information without their knowledge or consent if the disclosure is made to certain prescribed entities, including government institutions, health care institutions, post-secondary institutions, or public libraries in Canada.

It should be noted the CPPA explicitly states that several exemptions will not apply in certain circumstances where an individual's electronic address is collected or used (without their knowledge or consent) by unlawfully accessing a computer system.

Privacy Management Program

Organizations will be required to have a "privacy management program" that outlines the organization's policies, practices, and procedures for complying with privacy laws. The program must cover how the organization develops privacy management materials, protects personal information, manages requests for information and complaints, and trains and informs staff. Alternatively, organizations have the option to establish a "code of practice" or "certification program" that meets or surpasses the CPPA's requirements for safeguarding personal information and seek the Privacy Commissioner's approval of such code or program.

Right to Delete

Individuals have the right to request the "disposal" (deletion) of their personal data. There are exceptions, however, such as where the requested data cannot be separated from someone else's personal data or where an organization has a legal obligation to retain the information.

Right to Data Portability

Individuals will have the right to transfer their personal information to another organization. However, this transfer would be subject to a "data mobility framework" and future regulations, still to be developed under the CPPA.

Increased Protection for Minors

The information of minors will be classified as "sensitive information" and afforded increased protection.

Transparency on Automated Decisions

Organizations will have to provide, by request, a general explanation of the organization's use of any automated decision system to make predictions, recommendations, or decisions about

individuals that could significantly impact them.

New Powers and Penalties

Notably, the bill proposes to enhance the powers of the Privacy Commissioner and introduces new penalties (including significant financial penalties), as summarized below.

Privacy Commissioner's Enhanced Powers

The Privacy Commissioner will gain new powers, including:

- **Recommendation of Penalties:** The ability to propose large administrative monetary penalties for violations (as further described below).
- **Compliance Orders**: The power to issue compliance orders to bring organizations in compliance with the CPPA.
- **Corrective Measures:** The ability to access an organization's privacy program and recommend corrective measures.
- **Approval of Programs**: As noted above, the ability to approve, upon request, an organization's code of practice or certification program. The Privacy Commissioner can then monitor the implementation of the code or program and even revoke an approval of a certification program according to any prescribed criteria (to be set out in future regulations).

The Privacy Commissioner will also continue to maintain certain powers currently set out in PIPEDA, including the general ability to conduct inquiries (i) after investigating complaints; or (ii) if it suspects organizations are contravening compliance agreements, as well as conducting audits of an organization's compliance with privacy legislation.

Personal Information and Data Protection Tribunal

The new tribunal will be responsible for hearing appeals of findings and orders made by the Privacy Commissioner. It will also assess whether the Privacy Commissioner's recommended penalties are appropriate.

The tribunal will operate similarly to a court – a decision may be transformed into an order of the federal court or any superior court and hold the same enforceability as a court order. However, the tribunal's decisions can only be challenged through judicial review; they cannot be appealed.

New Penalties

The tribunal will be able to impose administrative monetary penalties (in reality, fines) of up to $10 million or 3% of the organization's gross global revenue from the previous fiscal year, whichever is higher.

The CPPA also introduces criminal offenses, such as failing to report breaches to the Privacy Commissioner, failing to maintain proper records, and obstruction. Other violations may include destroying records subject to access appeals, using anonymous information to identify individuals in unauthorized circumstances, engaging in reprisals, or obstructing an inquiry by the Privacy Commissioner. These offenses require proof that the organization knowingly committed the contravention. Organizations convicted of these offenses can be fined up to $25 million or 5% of the organization's gross global revenue, whichever is higher.

New Private Right of Action

Individuals will be able to sue organizations for injuries caused by a contravention of the CPPA. Class actions will be available and are a likely way that these actions will be commenced. However, before an individual can make a claim, an organization must have been found to have contravened the CPPA by the Privacy Commissioner or the tribunal.

Conclusion

Bill C-27's main goal is to establish "a regulatory framework that supports and protects Canadian norms and values, including the right of privacy" (as noted in the preamble). The bill will align Canadian privacy legislation with other jurisdictions, notably the European Union's GDPR.

To ensure compliance, businesses should be prepared to:

- Ensure there is a designated privacy officer informed of the upcoming amendments.
- Enforce and maintain clear and strong external and internal privacy policies across the organization.
- Review and maintain clear consent mechanisms that align with the upcoming amendments.
- Keep detailed records of consents and purposes for which personal information has been collected.
- Document any anonymization processes in detail to showcase the process's intended purpose and the efficacy in eliminating the ability to tie the information to an identifiable individual.
- Maintain a comprehensive record log of all privacy breaches.
- Notify legal counsel promptly if threats to the organization's privacy or data security are detected.

Ultimately, when Bill C-27 becomes law, business owners will have to assess their current business practices, privacy protection strategies, and existing policies in order to bring them into compliance.

Cozen O'Connor will closely monitor the bill's progress through parliament.

If you have any questions about this article or if you need assistance navigating privacy legislation, the Bill's amendments, or best practices, please feel free to contact the author, Any Obando Ospina, or any member of our Technology, Privacy & Data Security Group.