

Proposed Changes to Canada's Privacy Laws: What Organizations Need to Know

June 30, 2022

By , Vipal Jain

On June 16, 2022, Canada's federal government introduced the *Digital Charter Implementation Act* (Bill C-27). This Bill, if passed into law, would update Canada's federal private sector privacy law, establish a Personal Information and Data Protection Tribunal, and introduce new rules governing the use of artificial intelligence. Bill C-27 reintroduces Bill C-11, which was first introduced in 2020 but died on the order paper due to the 2021 federal election. Bill C-27 in its current form establishes three new statutes:

- *Consumer Privacy Protection Act* (CPPA);
- *Personal Information and Data Protection Tribunal Act* (DPTA); and
- *Artificial Intelligence and Data Act* (AIDA).

This article focusses on some key takeaways of Bill C-27 with respect to data privacy and its impact on organizations collecting personal information. The Bill as currently drafted, and similar to current Canadian federal private sector privacy legislation, applies to certain organizations located in Canada, and may also apply to organizations outside of Canada depending on the facts.

If Bill C-27 becomes law in its current form, it would replace the federal private sector privacy legislation that came into force 21 years ago (*Personal Information Protection and Electronic Documents Act* also known as PIPEDA) and result in significant changes to Canada's data privacy laws as described below.

- **Penalties:** CPPA establishes significant fines for non-compliant organizations. Organizations could face fines up to 5% of global revenue or \$25 million, whichever is greater, for offences such as failing to report privacy breaches to the Privacy Commissioner or destroying records which are subject to an access appeal. The upper limit of these fines exceeds those of GDPR and Quebec's Bill 64 (although the latter provides for doubled fines for repeat offenders). Additionally, organizations can face penalties up to a maximum of \$10 million or 3% of gross global revenue. These additional penalties apply to a variety of breaches of the CPPA, such as failing to dispose of personal information or not protecting it in a secure manner.
- **Enhanced Powers of the Privacy Commissioner:** Among the significant changes, the Privacy Commissioner would have the power to order organizations to change their data practices. The Privacy Commissioner would also have the power to recommend penalties to the new Personal Information and Data Protection Tribunal and approve an organization's code of practice or certification program to meet compliance requirements.
- **New individual Rights:**
 - **Deletion:** Currently, organizations are required to provide individuals with a right to access and correct their personal information, upon request, in certain circumstances. Bill C-27 also requires organizations to dispose, or in other words, delete an individual's personal information, upon request, when it is no longer needed.
 - **Data Mobility:** Bill C-27 would require organizations, upon request, to disclose personal information it has collected from an individual to another organization chosen by the individual if both organizations are subject to a data mobility framework.

- Automated Decision Systems: Bill C-27 would also require organizations, upon request, to provide an explanation about a prediction, recommendation, or decision made about an individual by automated means where it “could have a significant impact” on the individual.
- Policies and Privacy Management Program: Organizations are required to implement and maintain a privacy management program that includes policies, practices, and procedures to address, for example, the protection of personal information, how requests for information and complaints are handled, and staff training.
- Consent: While many of the consent requirements for the collection, use or disclosure of personal information would remain the same, Bill C-27 includes several additional exceptions to the requirement for consent. These exceptions include defined business activities, transfers to service providers, and prospective business transactions.
- New Tribunal: Bill C-27 creates a new Personal Information and Data Protection Tribunal, which would have the power to review certain decisions made by the Privacy Commissioner and impose penalties under the CPPA. Organizations may appeal a Privacy Commissioner decision to the Tribunal, which would have the authority to impose penalties. The Tribunal’s decision would be final and binding, and not subject to appeal or review by any court except in limited circumstances.
- Private Right of Action: Bill C-27 establishes a private right of action. Individuals would be permitted to bring an action against an organization for breaches of the CPPA. To commence such an action, certain conditions would need to be met. For instance, the alleged breach of the CPPA must be supported by a finding made by the Privacy Commissioner or the Tribunal. If the conditions are met, the individual would be entitled to damages for loss or injury suffered due to the breach.
- Anonymization and De-identified Information: Bill C-27 distinguishes between de-identified and anonymized information. “De-identify” in Bill C-27 means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains. On the other hand, “anonymize” in Bill C-27 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. Personal information that has been anonymized falls outside the scope of the CPPA.
- Protection of Minors: Bill C-27 contains new protections related to children’s privacy. It deems personal information of minors to be sensitive information.

The foregoing are a few of the many privacy law changes set out in Bill C-27. The list above is by no means exhaustive. The proposed changes set out in the initial Bill may or may not be reflected in the final version of Bill C-27.

Next Steps for Organizations

With numerous changes potentially expected in Canada’s data privacy landscape, organizations should consider how this affects the way they handle personal information. Given the exposure for serious liability under the CPPA, organizations should undertake a methodical review of their existing data management processes and policies, as well as data protection and privacy best practices to prepare for potential changes down the road.

If you have any questions, please contact the [Privacy & Access to Information](#) team.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

For more information or inquiries:

Toronto

Email:



Vipal Jain

Toronto

416.619.6294

Email:

vjain@weirfoulds.com

Vipal's practice focuses on privacy and technology matters. She advises organizations across various sectors on matters relating to privacy law compliance, technology contracting, cybersecurity incidents and artificial intelligence.

WeirFouldsLLP

www.weirfoulds.com

Toronto Office

4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110

Fax: 416.365.1876

Oakville Office

1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110

Fax: 905.829.2035