



## Canadian Tax & Legal Alert

### New cyber and privacy laws

*New risks, new compliance requirements*

July 18, 2022

The federal government recently introduced not one, but two new bills that will overhaul Canadian cybersecurity and privacy law, if passed. While these are exciting developments for privacy practitioners, the new legislation creates a host of obligations (which raise important questions) for critical infrastructure firms, corporations that collect, use and/or disclose personal information (PI), and private sector organizations that develop and employ artificial intelligence (AI).

#### Critical takeaways

- Bills C-26 and C-27 would create significant obligations for companies to implement plans to mitigate risk from cyber and privacy incidents.
- Mandatory breach reporting requirements are also included, which would create new national security considerations for critical infrastructure firms.
- Millions of dollars in daily monetary penalties could be imposed for ongoing violations.<sup>1</sup>

---

<sup>1</sup> A violation that is continued on more than one day would constitute a separate violation in respect of each day during which it is continued.

- Directors and officers could face personal liability for violations or offences under both Bills C-26 and C-27 (but a due diligence defence may be available).
- Regulators would have broad and enhanced investigative powers.
- New rules regarding AI development and implementation in the private sector would be tied to data protection, limiting biased output,<sup>2</sup> and significant monetary penalties in case of violation.
- As these bills have only just been tabled, industry stakeholders should have the opportunity to weigh in during the parliamentary committee stages.

## Overview of Bill C-26

Bill C-26, an **Act Respecting Cyber Security (ARCS)**, was tabled on June 14, 2022, to give the federal government broad powers over critical infrastructure sectors.

Part 1 of ARCS would amend the **Telecommunications Act** to empower the federal government to bar a specified product or service (or to remove a product) deemed to be a national security risk from being implemented in the telecommunications sector.

- Monetary penalties could be imposed for the violation of a security order of up to \$25,000 for an initial contravention for individuals (and up to \$50,000 for a subsequent contravention), and \$10,000,000 for organizations (and up to \$15,000,000 for a subsequent contravention).
- ARCS would also give the government authority to keep preparedness and response orders secret (e.g., to limit the disclosure of a telecom's cyber vulnerabilities).

Part 2 of ARCS would enact the **Critical Cyber Systems Protection Act (CCSPA)**, which provides further government authority over cybersecurity measures implemented by critical infrastructure operators, along with increased oversight when it comes to preparedness and reporting obligations. Additional obligations include the following:

- The CCSPA would require critical operators in four sectors – telecommunications, energy, finance, and transport – to immediately report incidents and breaches to the Canadian Centre for Cyber Security (which is part of the Communications Security Establishment).
- Regulators, including the Office of the Superintendent of Financial Institutions and the Bank of Canada, would have enhanced powers, such as on premise powers of entry as well as full audit authority with respect to an operator's cybersecurity systems (including documents and records).
- In addition, the CCSPA would require operators to establish robust cybersecurity programs that can detect serious threats and protect critical systems and keep records of how these systems were implemented to mitigate risk.
- Directors and officers of critical infrastructure organizations could also be found personally liable if their organization is in violation of the CCSPA; monetary penalties for individuals could reach up to \$1,000,000 per day; for organizations, monetary penalties of up to \$15,000,000 per day would be possible for ongoing violations.
- The specific list of entities affected by the new law is still being drafted. However, in a press briefing on June 14, 2022, the federal government

### Contacts:

#### [Hélène Deschamps Marquis](#)

National Data Privacy, Cybersecurity and Digital Law Practice Leader  
Partner, Deloitte Legal Canada  
Tel.: 514-393-8300

#### [Matt Saunders](#)

Associate Lawyer  
Deloitte Legal Canada  
Tel.: 902-425-2431

#### [Chetan Phull](#)

Associate Lawyer  
Deloitte Legal Canada  
Tel.: 416-874-3400

### Related links:

[Deloitte Tax Services](#)

[Deloitte Legal Canada LLP](#)

<sup>2</sup> *Biased output* means content that is generated, or a decision, recommendation or prediction that is made, by an artificial intelligence system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination set out in section 3 of the Canadian Human Rights Act, or on a combination of such prohibited grounds.

specifically named major Canadian telecommunications companies and rail companies as examples.

- The federal government will also be recommending that their provincial, territorial, and municipal counterparts consider drafting and implementing similar legislation.

## Overview of Bill C-27

Bill C-27, the **Digital Charter Implementation Act (DCIA)**, which was originally tabled in 2020, but not enacted before last year's federal election, was tabled on June 16, 2022. The DCIA is divided into three parts addressing (1) data privacy obligations, (2) administrative appeals, and (3) new AI rules.

Part 1 would enact the **Consumer Privacy Protection Act (CPPA)**, the federal government's second attempt at a new private sector privacy law intended to modernize the collection, use, and disclosure of PI in an ever-changing digital world. Key elements of the CPPA include the following:

- Organizations that collect, use, and disclose PI for commercial purposes would be required to implement a formal privacy management program (PMP), with designated resources and transparent, plain language policies for consumers.
- Organizations would also be required to assess the volume and sensitivity of PI under their control, ensure that consent from consumers is meaningfully obtained, and implement formal retention periods and access controls when it comes to protecting PI (e.g., reasonable authentication steps for employees).
- The federal privacy commissioner (OPC) would also have new order-making powers, including the ability to force a company to stop collecting data or using PI.
- The OPC would also be able to recommend a range of financial penalties for non-compliance, including administrative monetary penalties for failing to implement a PMP, failing to implement safeguards over the PI under an organization's control, etc. Penalties of up to 3% of global revenue or \$10,000,000 (whichever is greater) for these types of violations could be recommended.
- More severe offences, such as knowingly failing to report a data breach to the OPC, could result in penalties of up to 5% of global revenue or \$25,000,000, whichever is greater. However, defences of due diligence and reasonable efforts to mitigate harm would be available.
- The CPPA would define all PI of minors as sensitive information and require technology, media and telecom (TMT) companies that collect, use or disclose PI of minors to create specific messaging and consent notices for young consumers.
- Additional obligations would include having processes in place to deal with consumer requests to withdraw consent, move their PI to another organization, and delete PI on file.
- Organizations that use algorithmic decision-making tools (i.e., technology used in place of human decision-making), which could have a "significant impact" on an individual, would also be required to have processes in place to address consumer requests for information about these systems (e.g., the types of PI used, the source of the PI, the principal factors that led to the decision).

Part 2 would enact the **Personal Information and Data Protection Tribunal Act (PIDPTA)**, which would create an administrative tribunal (Tribunal) that will hear appeals from

certain decisions of the OPC, along with considering recommendations from the federal privacy commissioner to impose penalties on organizations in breach of the CPPA. Other key elements include:

- While the Tribunal would receive recommendations from the OPC, the PIDPTA would allow the Tribunal to substitute its own decision.
- There would be no right of appeal from a Tribunal decision; however, a party could apply for judicial review before the Federal Court.
- The Tribunal would be comprised of three to six full-time or part-time members, and at least three shall have experience in the field of information and privacy law.

Part 3 would enact the **Artificial Intelligence and Data Act (AIDA)**, which is intended to regulate international and interprovincial trade and commerce in AI systems.

Specifically,

- The new law would create several AI-related offences and violations, including improper use of PI, being reckless with AI likely to cause serious harm to individuals or substantial damage to property, and using AI to commit fraud.
- Penalties would be: up to \$25,000,000 or 5% of global revenue for organizations, and a discretionary fine and/or a term of imprisonment of up to five years for individuals.
- The question of whether any given AI is a “high-impact system” will be important. Future regulations will provide the definition. Until then, organizations should look to the EU AI Act<sup>3</sup> for guidance (based on past legislative practice in Canada; for example, Parliament previously used the EU AI Act’s four groups of AI risk classification in the Treasury Board Directive on Automated Decision Making)<sup>4</sup>.

## How can Deloitte help you?

As the impact of these proposed bills continues to unfold, Deloitte Legal’s national data privacy and cybersecurity team is happy to assist organizations prepare for and respond to these anticipated (and substantial) changes to Canada’s federal cyber and privacy law landscape.

---

<sup>3</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>

<sup>4</sup> This Directive sets out requirements that must be met by federal institutions to ensure responsible and ethical use of automated decision systems, including those using artificial intelligence (AI). (<https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>)



Deloitte LLP  
Bay Adelaide Centre, East Tower  
8 Adelaide Street West, Suite 200  
Toronto ON M5H 0A9  
Canada

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us on [LinkedIn](#), [Twitter](#), [Instagram](#), or [Facebook](#).

© Deloitte LLP and affiliated entities.

This document is intended to provide general information only. Accordingly, the information in this document is not intended to constitute accounting, tax, legal, investment, consulting or other professional advice or services. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional advisor. Deloitte makes no express or implied representations or warranties regarding this document or the information contained therein. Deloitte accepts no responsibility for any errors this document may contain, whether caused by negligence or otherwise, or for any losses, however caused, sustained by any person that relies on it. Your use of this document is at your own risk.

To no longer receive emails about this topic please send a return email to the sender with the word "Unsubscribe" in the subject line.