

2023 OSLER LEGAL OUTLOOK

The wave of privacy and data legislation reform will continue in 2024



DECEMBER 11, 2023 9 MIN READ

Related Expertise

- [Privacy and Data Management](#)
- [Privacy and Data Security Disputes](#)

Authors: [Adam Kardash](#), [Maryna Polataiko](#)

There are clear signals that privacy and artificial intelligence (AI) will continue to be focal points in the highly dynamic Canadian privacy arena in 2024. Over the course of 2023, a federal government proposal for a new private sector privacy law and a proposed framework for the regulation of AI continued their progression through the parliamentary process. The enactment of these new privacy and AI laws in 2024 or early 2025 appears increasingly likely.

Companies conducting business in Québec will need to continue their efforts to comply with multiple new and prescriptive compliance requirements under the *Act respecting the protection of personal information in the private sector* (the Québec Privacy Act), which was significantly reformed by the adoption of Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* [PDF] (Law 25). The majority of Law 25's amendments came into force in September 2023. These include an enforcement regime that exposes companies to potentially severe financial penalties for contraventions.

It is more important than ever for companies doing business both in Québec and across Canada to have a thorough understanding of their personal information and data practices and their obligations under these updated and pending laws. These amended and incoming statutory frameworks require companies across Canada to incur substantial compliance costs to mitigate the risks of severe penalties. Companies will need to identify and address the expanding array of privacy, legal, ethical and reputational risks associated with the collection, use and disclosure of personal information and the use of AI systems.

Québec's privacy legislative reform is now in force

The vast majority of Law 25's amendments to the Québec Privacy Act came into effect in September 2023.

These include a significantly enhanced enforcement regime bolstered by potentially severe financial penalties. Failure to comply with the Québec Privacy Act will expose organizations to fines of up to the greater of C\$25 million and the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. Non-compliance can also expose organizations to administrative monetary penalties of up to the greater of C\$10 million and the amount

corresponding to 2% of worldwide turnover for the preceding fiscal year.

Under the Québec Privacy Act, companies carrying on business in Québec must comply with a range of new and onerous requirements that have now come into force. These changes add to the security breach notification regime and rules relating to biometrics introduced under Law 25 that came into force in 2022, as we discussed in our [2022 Legal Year in Review](#) article.

Key obligations that came into effect in September 2023 include requirements for organizations to create an internal policy suite to address the lifecycle of personal information in their custody and control. Organizations must also conduct privacy impact assessments for any project involving the acquisition, development or overhaul of an information system or electronic service delivery system that entails the processing of personal information.

The Québec Privacy Act now contains prescriptive consent requirements for the collection, use and disclosure of personal information. In late October 2023, Québec's privacy regulatory authority, the Commission d'accès à l'information (the CAI), issued detailed guidance setting out its [Criteria for Valid Consent](#) [PDF]. Organizations will need to carefully consider this CAI guidance and examine the lawful basis for their collection, use and disclosure of personal information. Organizations will need to update their consent notices and develop or enhance consent management practices to ensure they are lawfully processing personal information.

Under Law 25's novel "confidentiality by default" requirements inspired by the concept of "privacy by design" under the EU's General Data Protection Regulation (GDPR), organizations must implement the "highest level" of confidentiality by default with respect to public-facing products or services. These requirements raise practical questions as to how organizations can be expected to comply.

The Québec Privacy Act also now contains a unique profiling requirement. Specifically, organizations collecting personal information from individuals using technology that allows those individuals to be identified, located or profiled must first inform the individual of such technology and of the means available to activate such functions.

Under Law 25's data localization restrictions, organizations have to create an inventory of all cross-border disclosures and transfers to meet requirements relating to transfers of personal information outside of Québec. Organizations are now required to conduct a privacy impact assessment prior to any disclosure of personal information outside Québec to ensure that the personal information will be "adequately protected" in the other jurisdictions. Organizations are prohibited from transferring or disclosing personal information outside the province of Québec where such information will not receive "adequate protection." This must be determined in light of "generally recognized principles regarding the protection of personal information."

Given these new obligations, organizations carrying on business in Québec will need to focus on satisfying compliance obligations to mitigate risks of potentially severe penalties.

Sweeping privacy legislative reform and proposed AI regulation are progressing

Legislation introduced in mid-2022 by the Canadian federal government will have a significant impact on the regulation of personal information and create a statutory

framework for the regulation and use of AI systems. These reforms are continuing to make their way through Parliament. It appears increasingly likely that these new laws will be enacted in the near future with critical implications for businesses in Canada.

Bill C-27 sets out the *Digital Charter Implementation Act, 2022* which creates a new statutory framework governing personal information practices in the private sector. The bill is currently before the Standing Committee on Industry and Technology (INDU) and may be passed in 2024 or early 2025. If enacted, Bill C-27 will establish three new statutes.

The first is the *Consumer Privacy Protection Act* (CPPA). This would repeal and replace the private sector personal information protection framework in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

In addition, the *Personal Information and Data Protection Tribunal Act* would establish an administrative tribunal to review certain decisions made by the Privacy Commissioner of Canada and impose penalties for contraventions of the CPPA.

Finally, the *Artificial Intelligence and Data Act* (AIDA) would create a risk-based approach to regulating trade and commerce in AI systems.

CPPA introduces new privacy regime

The new privacy regime introduced under the CPPA would replace PIPEDA. It contains a suite of new requirements governing the protection of personal information and proposes a substantially enhanced enforcement regime.

Failure to comply with the CPPA could expose organizations to fines of up to the greater of C\$25 million and the amount corresponding to 5% of gross global revenue for the preceding fiscal year. Organizations could also be exposed to administrative monetary penalties of up to the greater of C\$10 million and the amount corresponding to 3% of gross global revenue for the preceding fiscal year.

Among other key features of the draft CPPA is a requirement for organizations to implement a privacy management program, which must include policies, practices and procedures to fulfill the organization's compliance with the statute.

The CPPA reinforces consent, especially express consent, as the primary authority for organizations to process personal information. However, the CPPA also clarifies and creates new exceptions that authorize the collection, use or disclosure of personal information without such consent. These exceptions apply to certain defined standard business activities or where the organization has a legitimate interest, subject to certain conditions.

The CPPA includes numerous provisions relating to the lawful processing of "de-identified" data and "anonymized" data. The proposed provisions clarify that anonymized information is beyond the scope of the CPPA. The draft legislation also creates a special status for personal information of minors.

In certain circumstances – namely, where there could be a "significant impact" on individuals – the CPPA would require businesses to explain how a prediction, recommendation or decision was made by an automated decision-making system. Further, on request from a person, the business would be required to provide an explanation about the type and source of personal information used to make the prediction, recommendation or decision.

Furthermore, individuals would be able to request that organizations dispose of their

personal information. In certain circumstances, organizations would be required to comply with such requests. Finally, the CPPA includes provisions granting individuals data mobility rights, allowing them to direct the transfer of their personal information from one organization to another.

AIDA regulates creation and use of AI

Bill C-27 would also enact the AIDA, the first law in Canada regulating the creation and use of artificial intelligence systems. If enacted, the AIDA would create a significant penalty regime. This includes fines for contravention of up to 3% of global revenue or C\$10 million and fines of up to 5% of global revenue or C\$25 million for more serious offences, or imprisonment, in the case of an individual.

Key elements of the proposed framework for regulating AI systems include mandatory assessments to determine whether an AI system is a “high-impact system,” a term to be defined in the regulations. Organizations would be required to publish a description and explanation of each high-impact system and must mitigate the risks of harm or biased output from the use of such system.

The AIDA creates self-reporting requirements for organizations. It also introduces ministerial powers to order production of records, conduct an audit, publish warnings and order the cessation of use or distribution of a high-impact system. The AIDA further contemplates the appointment of an Artificial Intelligence and Data Commissioner to assist in the administration and enforcement of the legislation.

In October 2023, the Department of Innovation, Science and Economic Development Canada (ISED) issued [Canada’s Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems](#). This Code is framed as a “critical bridge” between now and the time when the AIDA comes into force. The proposed Code of Practice outlines organizational commitments to various core elements in the development, use and operation of generative AI systems. These are safety, fairness and equity, transparency, human oversight and monitoring, validity and robustness, and accountability.

While the Code of Practice is voluntary in nature, we anticipate it will be referenced by organizations across various Canadian industries in the development and management of AI systems. Additional information regarding how organizations can mitigate risks and navigate an increasingly complex regulatory environment directed at AI can be found in our article, [*AI governance: navigating the path ahead*](#).

If enacted, the requirements under Bill C-27 will impose significant obligations on organizations carrying on business in Canada. While these proposed legislative reforms remain subject to amendment, businesses are encouraged to begin planning for these requirements which will likely come into force in the coming years.