UNPACKING ONTARIO'S PROPOSED STRENGTHENING CYBER SECURITY AND BUILDING TRUST IN THE PUBLIC SECTOR ACT, 2024

Posted on May 17, 2024

Categories: Insights, Publications

On May 13, 2024, the Ontario government, spearheaded by the Minister of Public and Business Service Delivery, introduced Bill 194: the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (the "**Proposed Legislation**") to the Ontario Legislative Assembly.[1]

The stated objective of the Proposed Legislation is to enhance digital security and establish trust across public sector institutions, which include entities covered under the *Freedom of Information and Protection of Privacy Act*[2] and the *Municipal Freedom of Information and Protection of Privacy Act*[3], as well as children's aid societies and school boards.

The compliance impact of the Proposed Legislation would be felt directly by Ontario's public sector but also indirectly by companies that do business with Ontario's public sector.

The Proposed Legislation encompasses amendments to existing legislation and introduces new regulatory frameworks focused on cyber security, the use of artificial intelligence ("**AI**"), and the management of digital information concerning minors. This bulletin provides an overview of key provisions of the Proposed Legislation and considers potential implications for covered public sector entities and their private sector partners.

Introduction of the *Enhancing Digital Security and Trust Act, 2024*

Schedule 1 of the Proposed Legislation introduces a proposed new law, labelled the *Enhancing Digital Security and Trust Act, 2024* (the "**Proposed EDSTA**"). As set out further below, the Proposed EDSTA would impose on public sector entities: (1) cybersecurity standards to be prescribed by regulation; (2) an AI governance framework; and (3) restrictions relating to the processing of personal information about minors.

- **Cyber Security Regulations.** The Proposed EDSTA would empower the Lieutenant Governor in Council to establish sector-specific cyber security regulations. The cyber security provisions do not set out specific requirements, but indicate that the regulations could include mandatory development and implementation of cyber security programs, cyber security incident reporting, and adherence to

prescribed technical standards. The Proposed EDSTA would also authorize the Minister to set technical standards and issue directives regarding mandatory cyber security measures.

Notably, the cyber security incident reporting regime contemplated by the Proposed EDSTA would be different from and in addition to mandatory personal information breach reporting discussed further below.

- **AI Framework.** The Proposed EDSTA would apply to the use or intended use of AI systems by public sector entities. Specifically, the requirements would require prescribed public sector entities to disclose information about the use of AI systems, develop an accountability framework and comply with additional requirements prescribed by regulation (including those relating to risk management).

  The proposed definition of an "AI system" that would fall within the scope of the Proposed EDSTA is: "a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments" with the opportunity for additional systems to be prescribed by regulations.

- **Protection of Minors' Digital Information.** The Proposed EDSTA would empower the Lieutenant Governor in Council to establish regulations pertaining to prescribed children's aid societies and school boards. As with the cyber security provisions referenced above, the Proposed EDSTA does not impose specific requirements, but indicates that the regulations could include prescribing the way digital information about minors can be processed, imposing reporting requirements for covered institutions that process such information and, in certain circumstances, prohibiting the processing of such information altogether.

  In addition to the above, the Proposed EDSTA would also authorize the Minister to set technical standards and issue directives regarding personal information about minors as well as digital technology that may be made available for use by minors.

Amendments to the *Freedom of Information and Protection of Privacy Act*

Schedule 2 of the Proposed Legislation would introduce amendments to Ontario's *Freedom of Information and Protection of Privacy Act* ("**FIPPA**"). FIPPA, among other things, governs the processing of personal information by public sector entities in Ontario. Notably, the Proposed Legislation does not impose any changes to FIPPA's municipal counterpart, Ontario's *Municipal Freedom of Information and Protection of Privacy Act*.

The proposed amendments seek to modernize FIPPA by mandating the conduct of privacy impact assessments ("**PIA**") and personal information breach reporting and by enhancing the oversight powers of the Information and Privacy Commissioner of Ontario (the "**Ontario IPC**").

- **Mandatory PIAs.** The Proposed Legislation amends FIPPA to introduce a mandatory requirement that public entities conduct a PIA prior to collecting personal information, which must set out specified information regarding the public entity's processing and protection of such information. The amendment would also require updates to the PIA before using or disclosing personal information for a new purpose.

  The statutory requirement to conduct a PIA would bring Ontario in line with other provincial/territorial jurisdictions statutorily mandating PIAs for public sector entities in certain circumstances, such as British Columbia, Quebec, Newfoundland & Labrador, and the three Territories.

- **Mandatory Breach Reporting and Notification.** The Proposed Legislation amends FIPPA to impose an express obligation on public sector entities to take reasonable steps to safeguard personal information from theft, loss and unauthorized use and disclosure, along with a mandatory obligation to notify the Ontario IPC and affected individuals of breaches of such safeguards that result in the familiar "real risk of significant harm" threshold. The draft amendment would also allow additional reporting thresholds to be added by regulation.
- **Enhanced Oversight and Enforcement Power for the Ontario IPC.** The Proposed Legislation enhances the oversight and enforcement powers of the Ontario IPC by formalizing its ability to conduct a review of the information practices of a public entity on the basis of a complaint or its own initiative, and to make orders in connection with such reviews.

  In addition to the above, the Proposed Legislation would introduce protection for whistleblowers who report information regarding non-compliance with a public entity's obligations under FIPPA.

Next Steps

The Proposed Legislation will affect public sector entities and, indirectly, their private sector partners. Both the Proposed EDSTA and amendments to FIPPA have the potential to significantly change the regulatory landscape regarding the processing of personal information by Ontario's public sector, with the opportunity for new requirements to be introduced periodically by way of regulation going forward.

The Ministry of Public and Business Service Delivery is accepting comments from interested stakeholders until June 11, 2024.

For a detailed analysis of how the Proposed Legislation may affect your operations, or to obtain further information and assistance regarding participation in the public consultation process, please contact McMillan LLP's Privacy & Data Protection Group. We are committed to providing you with tailored advice that ensures your data protection strategies are both compliant and effective in this forthcoming regulatory era.

[1] Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 - Legislative Assembly of Ontario (ola.org); Ontario Strengthening Cyber Security and Protecting People Online | Ontario Newsroom.
[2] *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31.
[3] *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56.

By Mitch Koczerginski and Stephen Johnson

A Cautionary Note