Bulletin | Cybersecurity, Privacy and Data Protection

February 2022

Special committee recommendations to modernize B.C.'s private sector privacy law

In December 2021, a special committee appointed by the Legislative Assembly published a report recommending significant changes to British Columbia's *Personal Information Protection Act*. In light of the report and other developments in domestic and international privacy laws, private sector organizations should now take steps to prepare for compliance with significantly amended privacy laws in British Columbia.

Introduction

British Columbia's *Personal Information Protection Act* ("**PIPA**") governs how provincially-regulated private sector organizations (including businesses and non-profit organizations) collect, use, disclose and retain personal information of individuals (including employees and members of the public) within British Columbia. PIPA came into force in 2004 and was recognized by the federal government of Canada to be "substantially similar" to comparable provisions in the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), which allows provincially-regulated private sector organizations in British Columbia to comply with PIPA (instead of PIPEDA) regarding the handling of personal information within British Columbia.

PIPA is subject to mandatory periodic reviews by a special committee of the Legislative Assembly, which is required to submit a report that may include recommended amendments to the statute. Special committee reports in 2008 and 2015 included recommendations for numerous changes to PIPA that the Legislative Assembly did not implement.

In April 2021, the Legislative Assembly appointed a special committee to review PIPA (the "**Special Committee**"). In December 2021, the Special Committee published a report titled *Modernizing British Columbia's Private Sector Privacy Law* (the "**Report**") with 34 recommendations for significant changes to PIPA. The Special Committee concluded that "PIPA must be modernized to safeguard rights for individuals and provide up-to-date provisions to ensure competitiveness for British Columbia's businesses".

The Information and Privacy Commissioner for British Columbia (the "**Privacy Commissioner**") announced his support for the Report, explaining that the recommendations in the Report "chart a way forward to strengthen the protection of the public's personal information while fostering innovation on the part of BC business in this increasingly technology driven world". The British Columbia government has not issued a formal response to the Report.

Summary of key recommendations

Following is a summary of some of the Special Committee's recommendations for amendments to PIPA:

- **Alignment/harmonization:** Align PIPA with the "gold standard" privacy principles in the European Union's *General Data Protection Regulation* and anticipated amendments to PIPEDA, and harmonize PIPA with other Canadian provincial and international privacy legislation.
- **New/emerging issues:** Specifically address new and emerging issues, such as de-identification and re-identification of data, automated decision-making, and biometrics.
- **Consent:** Reinforce the foundational principle of meaningful consent, require explicit consent for specified categories of sensitive information (e.g., biometric data, medical information, and information about children/youth), align consent exceptions with those in the European Union's *General Data Protection Regulation*, and require explicit consent for the sale of personal information.
- **Breach notification:** Require organizations to notify the Privacy Commissioner and affected individuals of a privacy breach, with consideration for proportionality regarding the severity of the breach.
- **Data portability:** Give individuals a right to obtain their personal information in a structured, commonly used, and machine-readable format.
- **Data retention/destruction:** Define data destruction requirements and require organizations to outline their data retention periods and data destruction methods in their privacy policies.
- **Privacy impact assessments:** Require organizations to conduct privacy impact assessments for new projects involving high-risk sensitive information.
- **Data controllers/processors:** Confirm that data controllers are responsible for the personal information they transfer to data processors, and require data controllers to use contractual or other means to ensure PIPA compliance.
- **Employees:** Strengthen the protection of employee privacy and address the use of employees' personal devices in the workplace.
- **Health information:** Create new legislation for health information in the public and private sectors.
- **Enforcement:** Enhance the Privacy Commissioner's enforcement powers, including powers to conduct audits/investigations, issue findings/orders, enter into compliance agreements, and impose administrative monetary penalties (i.e., fines) that are proportionate to the PIPA violation and sufficient to deter PIPA contraventions.

Comment – Preparing for compliance

In light of significant developments in domestic and international privacy laws – including amendments to British Columbia's *Freedom of Information and Protection of Privacy Act*, Québec's adoption of *Bill 64, An Act to modernize legislative provisions as regards the protection of personal information*, and amendments to PIPEDA contemplated by the federal government's *Digital Charter* – and the need for PIPA to remain "substantially similar" to PIPEDA, one may confidently predict that PIPA will soon be amended to implement the substance of many of the Special Committee's recommendations. See BLG bulletins *Changes to B.C.'s public sector privacy legislation* and *Québec adopts Bill 64 – Key requirements for businesses*.

Consequently, private sector organizations that handle personal information within British Columbia should now begin to take steps to prepare to comply with an amended PIPA that implements the Special Committee's recommendations. Following are some suggestions:

- **Mandate/budget:** Ensure the organization's senior management understands the implications of recommended PIPA amendments (including enhanced Privacy Commissioner investigation and enforcement powers), and approves the work required for compliance with the amendments.
- **Data handling assessment:** Understand and assess the organization's current personal information handling practices, including preparing detailed and comprehensive data maps.

- **Personal information governance framework:** Collect the organization's current personal information policies and procedures (including incident response plans, breach notification guidelines, privacy impact assessment forms, and BYOD policies), and assess them for accuracy, suitability and compliance with current and anticipated legal requirements, regulatory guidance and recommended best practices.
- **Material contracts:** Review the organization's material contracts with service providers and other organizations (including affiliates) that handle personal information on behalf of the organization, and prepare to amend those agreements when possible. Ensure that new contracts include provisions allowing for legal compliance amendments.
- **Implementation planning:** Start planning for the internal implementation of new policies/procedures and data handling practices, including required employee education and training.
- **Systems/services:** Consider whether the organization must update or replace its internal systems and external services to comply with PIPA amendments (including requirements for safeguarding personal information), and plan accordingly.
- **Privacy by design:** Implement privacy by design in all new programs and business arrangements.

When preparing for compliance with an amended PIPA, organizations should be mindful of restrictions/requirements imposed by other applicable laws regarding the handling of personal information and the procurement and use of information technology systems and services. See BLG bulletins *BCFSA finalizes information security and outsourcing guidelines*, *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*, *Frequently Asked Questions – Compliance with PIPEDA's Security Breach Obligations* and *IIROC Imposes Mandatory Reporting of Cybersecurity Incidents for Regulated Investment Firms*. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Danielle Windt
T 604.640.4120
dwindt@blg.com

BLG's national Compliance with Privacy and Data Protection group includes lawyers, located in BLG's offices across Canada, with expertise in Canadian and international privacy laws, cyber risk management and class action litigation. We provide both proactive compliance advice and legal advice to help respond to a privacy breach or resolve privacy disputes. Additional information about BLG's national Compliance with Privacy and Data Protection group and our services is **available here**.