Castra Technologies

Cybersecurity and Data Privacy Experts

Canadian Privacy Legislative Update – August 6, 2024

CastraTech.com

Canadian Provinces

PIPEDA – Canada Federal Law

- Applies to both consumer and employee information
  - See full Canada Privacy Analysis*
- Federal Bill C-27 progress would update PIPEDA to keep pace changes in GDPR. However, it is not expected to pass in 2024.
  - Clarified consent requirements for the collection, use and disclosure of PI
  - Expanded enforcement powers of the Privacy Commissioner
  - Align fines with GDPR up to 5% of annual gross revenue or CA$25M
  - New rules governing de-identified information

Bill C-27 Introduced June ‘22 to Replace and Supplement PIPEDA

- **Consumer Privacy Protection Act (CPPA).** Set to replace Part 1 of PIPEDA but keep Part 2 to provide a means to communicate or record information or transactions or the “Electronic Documents Act”.
  - Stronger fees up to $10 million CAD or 3% of global revenue, with negligence reaching $25 m CAD or 5% of revenue.
  - New Right of Action for individuals who suffer losses or injuries as a result of a CPPA violation.
  - Organizations must implement a privacy management program, with risk factors for data volume and PI sensitivity.
  - Have documented privacy policies, practices, and procedures.
  - Explicit Consent but with many exceptions (likely to be modified before passage).
  - Clarifying de-identification and anonymized Personal Information. Anonymized is the way to go… “to irreversibly and permanently modify personal information" such that it is impossible to reidentify them according to "generally accepted best practices”.
  - Right to request disposal of their PI and organizations must ensure sub-processors and service provider do likewise. De-identification is an acceptable method of disposal.
  - Right of data portability.
- **New Tribunal (PIDPTA).** Create a new administrative tribunal to review decisions made by the Privacy Commissioner of Canada, hear appeals and impose penalties.
- **Artificial Intelligence and Data Act (AIDA).** AI systems used to predict, recommend, or make a decision on an individual, must be explained to the individual.

Quebec Law 25

- Previously Bill 64, effective September 22, 2022
- In addition to new individual rights over their Personal Information, the law requires:
  - Breach Notification
  - Privacy Notices
  - Appointment of a Data Protection Officer
  - Consent Before Processing
  - Restriction on PI of a minor (<14)
  - Data Minimalization
- Mandates risk assessments (PIA) before data can be transferred external to Quebec. Similar to GDPR requirements on data movements outside the province, including to other Canada provinces and the US.
- Appointment of a DPO, similar to GDPR.
- Applies to both consumer and employee information.

Law 25 (Bill 64) Privacy Sector Act – Effective September 22, 22

- **Breach Reporting.** Organizations must notify CAI and impacted individuals of unauthorized access to personal information that poses “real risk of significant harm” under PIPEDA.
- **Breach Register.** Organizations must keep a register of all breaches.
- **Data Protection Officer.** Organizations must designate an employee responsible for complying with data privacy laws and publish the name, title, and contact information of the individual on their website.

Law 25 – Requirements Effective September 22, 2023

- **Individual Rights.** Individuals have a right to be forgotten and to data portability. This includes the right of access or rectification within 30 days.
- **Public Disclosures and Notices.** Organizations must publish notices their website for personal information.
- **Privacy Impact Assessments (PIAs).** Must conduct an assessment of privacy risks or "any information system or electronic service delivery project involving the collection, use, communication, keeping or destruction of personal information."
- **Consent and Disclosures.** Consent must be clear, free, and informed and for a specified purpose. Before personal information is collected, used, or released, organizations must request consent separately from any other information provided to the individual. Organizations must provide details of the purpose for collection, the categories of information, the means used for collection, the duration of time that the information will be kept, and the individuals' rights related to the information.
- **Enforcement.** CAI has the power to issue monetary penalties, up to maximum amount is CAD $10 million or, if greater, 2% of global revenue. For penal offenses, CAI may issue a maximum fine of CAD $25 million or 4% of global revenue.
- **Cross-border flows of data**. Requires restrictive provisions for the flow of data outside of Quebec and the transfer to third-party processors. PIAs must be conducted prior to the release of personal information outside of Quebec.
- **Privacy by Default.** Organizations must implement privacy options as "on" by default.

Alberta & British Columbia Personal Information Protection Act

PIPA-AB

- Updated 2014.
- Applies to consumers and employees
- Limitations on use
- Limitations on disclosure
- Limitations on collection
- Core rights of access, correction, accuracy
- Limits on retention
- Requires protection of the information

- Requires Consent to collect and process.
- Requires appointment of DPO or other person responsible for compliance with the law.
- Breach notification, including breach registry

PIPA-BC

- Dates to 2003 with periodic, minor updates.
- Applies to consumers and employees
- Limitations on use
- Limitations on disclosure
- Limitations on collection
- Core rights of access, correction, accuracy
- Limits on retention
- Requires protection of the information