Bill 64 on modernizing Québec privacy law

Why it matters and how to prepare for it

Part 1 presented on October 14, 2021

大成 DENTONS

Speakers

Chantal Bernier
Counsel, Ottawa
chantal.bernier@dentons.com

Chantal Bernier leads Dentons' Canadian Privacy and Cybersecurity practice group. She is also a member of the Firm's Government Affairs and Public Policy group.

Chantal advises leading-edge national and international companies as they expand into Canada and Europe, enter the e-commerce space, adopt data analytics and roll out data-based market initiatives.

Her clients include ad tech companies, financial institutions, biotech companies, data analytics firms and government institutions.

Alexandra Quigley
Senior Associate, Montréal
alexandra.quigley@dentons.com

Alexandra Quigley is a member of the Litigation and Dispute Resolution group in Dentons' Montréal office. Her practice focuses on civil and commercial litigation.

Alexandra has carried out various civil and commercial litigation mandates and has appeared before the Court of Québec, the Superior Court and the Court of Appeal.

She also advises clients in privacy matters and is completing a masters in information technology law at the Université de Montréal.

Agenda

1. Why Bill 64 matters beyond Québec
2. The Game Changer: Financial Risk
3. Increased obligations
4. New rights for individuals
5. Regulation of de-identified and anonymized data
6. Needed organizational changes
7. 5 lessons learned from reviewing Privacy Programs

The importance of Bill 64

Bill 64 applies in Québec and has cross-border impacts

- The Commission d’accès à l’information (CAI) regularly exercises its competence, even on organisations governed by PIPEDA

- Bill 64 creates a unique precedent in Canada that may be reflected by other provincial legislative reforms

The game changer: Financial Risk

1. Administrative monetary penalties

The CAI can impose administrative monetary penalties of up to $10M or 2% of the organisation’s worldwide turnover

Violations

- Refuse to communicate information in accordance with the transparency obligation pertaining to the processing of personal information
- Processing personal information in violation of the Act
- Failure to report a confidentiality incident to the CAI or to the persons concerned
- Failure to take appropriate security measures to ensure the protection of personal information
- Refusing to inform the person concerned by a decision based exclusively on an automated process
- Failure to meet the obligations imposed on a personal information agent under the Act

2. New penal offences and fines

Courts may impose fines of up to $ 25M or 4% of the worldwide turnover

Violations:

- Processing personal information in violation of the Act
- Failure to report a confidentiality incident posing a risk of serious harm to the CAI or to the persons concerned
- Requesting personal information despite a security freeze
- Identifying or attempting to identify a natural person using de-identified information, without authorization
- Failure to adequately protect personal information
- Failure to meet the obligations imposed on a personal information agent under the Act
- Impeding a CAI investigation
- Retribution against a complainant or a person collaborating with the CAI
- Refusing to produce documents requested by the CAI or to respect an order rendered by the CAI

Private right of action

Courts will award punitive damages of “no less than $1,000” in cases where the infringement is intentional or results from gross negligence

Violations:

- Rights conferred by the Act
- Rights conferred by articles 35 to 40 of the Québec Civil Code

Increased obligations

1. Breach Reporting

Reporting Obligations

- Organisations must inform the CAI and the affected individuals when the confidentiality incident presents a risk of serious injury
- Keep a registry of breaches
- Provide the registry to the CAI upon request

Post-reporting Obligations

- Decrease the risk of injury
- Prevent subsequent breaches of the same nature

Breach incident:

- Unauthorized access, use or communication;
- Loss; or
- Any other beach in the protection of personal information

Serious injury is assessed according to:

- The sensitivity of the information concerned;
- The anticipated consequences; and
- The likelihood that the information will be used for harmful purposes.

2. A robust governance structure

Ensuring compliance with the Act:

- By default, the “person exercising the highest authority” will be responsible to ensure compliance with the Act
- This responsibility can be delegated to a Data Privacy Officer (DPO)
- The Data Privacy Officer’s contact information must be made public

2. A robust governance structure (continued)

Policies and practices:

- Organisations must implement policies and practices concerning the protection of personal information
- These policies and practices must be proportional to the nature and the importance of the data being processed
- They must be approved by the Privacy Officer
- They must be available on the organisation’s website

Under the Act, policies and practices must establish:

- The framework for the conservation and the destruction of personal information
- The roles and responsibilities of personnel throughout the life cycle of the personal information
- A procedure to review and assess complaints regarding protection of personal information

3. Consent

- Consent must be clear, free and informed
- Consent must be given for specific purposes
- Consent must be obtained for each purpose for which personal information is collected
- Where the personal information is sensitive, consent must be given expressly
- Implicit consent only applies in certain situations
- Personal information is sensitive if, due to its nature, including medical, biometric or otherwise intimate information, or the context, it entails a high level of reasonable expectation of privacy
- A request for consent must be separate from other information provided to the individual
- Consent of a minor under 14 years of age must be given by the person having parental authority or the tutor

3. Consent (continued)

Cases where personal information may be used without the consent of the individual concerned:

- If it is used for purposes consistent with the purposes for which it was collected
- If it is clearly used for the benefit of the individual concerned
- When necessary to prevent and detect fraud, or to improve protection
- When necessary to supply a product or to deliver a service
- When used for study or research purposes or to produce statistics, if the information is de-identified

4. Transparency

- Transparency is ensured by publishing information regarding privacy protection policies and practices
- The privacy policy must be published on the organisation’s website
- The privacy policy must be drafted in clear and simple terms

The following information must be divulged upon collection:

- The purposes
- The means
- The rights of access and rectification, and
- The right to withdraw consent

5. De-identification and anonymization

“De-identified” information: the information can no longer be used to directly identify the concerned person

“Anonymized” information: the information can no longer and irreversibly be used to directly or indirectly identify the individual concerned

- The right to use information varies according to the type of information
- The use of de-identified information is subject to restrictions in order to protect against re-identification
- The use of anonymized information is subject to generally accepted best practices

New Rights for Individuals

1. Data portability

- An individual has a right to request their personal information be communicated to them or to a designated third party
- The information must be provided in a structured and commonly used technological format
- This right will come into effect in three years, from September 22, 2021

Exceptions:

- The request may be refused if it causes serious difficulties
- The data portability right does not extend to information created or inferred from the concerned individual’s personal information

2. Right to be forgotten

- Right to request that an organisation cease dissemination personal information
- Right to request that personal information be de-indexed
- Right to request that inaccurate, incomplete or incorrect information be rectified

Conditions:

- The dissemination of the information causes the person concerned serious injury in relation to their right to respect of their reputation or privacy;
- The injury caused is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing themselves freely; and
- The cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury

3. Automated Processing

- Organizations must inform the individual when his or her personal information is used to render a decision based exclusively on an automated processing of such information
- Automated processing refers to the use of personal information without human intervention
- The concerned person is entitled to submit observations regarding the decision

Upon request, an organisation must inform the individual concerned of:

- The personal information used
- The reasons for and the principal factors and parameters that led to the decision
- Their right to have the personal information used amended to render correct the decision

Needed Organizational Changes

Trending: the strengthening of accountability obligations leading to structural changes

The European General Data Protection Regulation (GDPR) (2018):

- Mandatory appointment of a data protection officer for certain companies
- Record of processing activities
- Mandatory data protection impact analysis for certain initiatives

Bill C-11:

- Incorporates the National Standard of Canada titled *Model Code for the Protection of Personal Information*

Bill 64 is part of the same process:

- Data Privacy Officer
- DPO practice requirements

1. Review of Privacy Program

Do you have a Chief Privacy Officer (CPO)? If so,

- Are you sure the CPO is at the right level? Take into account:
  - Their expertise;
  - Their authority – to compel compliance;
  - Their independence – to put in place policies and practices and to avoid conflicts of interest.

Do you have an Incident Response Plan? If so:

- Does it meet Bill 64’s requirements?
- Has it been communicated to employees?

1. Review of Privacy Program (continued)

Do you have an inventory of your databases?

- What type of data do you hold?
- How do you use them and for what purpose?
- Do they include sensitive personal information?

Do you have practices and procedures to ensure PPI?

- On limitation of collection?
- On limitation of use?
- On the nature and form of consent to receive?
- On retention schedules?
- On protection of personal information?
  - Getting Accountability Right with a Privacy Management Program

    (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic- documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204)

2. Developing new procedures:
2.1 Privacy Impact Assessment (PIA)

- For any information system or electronic service delivery project involving the processing of personal information;

- Before transferring personal information outside of Québec; and

- Before disclosing personal information without the consent of the persons concerned for the purposes of study, research or production of statistics

Implementation:

- Determine necessity criteria
- Assign responsibility
- Procedure for consulting the person responsible for PI
- Adopt an analytical model
- Establish a development and approval process

- Treasury Board Secretariat Directive on Privacy Impact Assessment

2.2 PIA for transfer of personal information outside of Quebec

Context:

- The Office of the Superintendent of Financial Institutions already requires privacy due diligence from financial institutions
- The OPC adopted the same requirement in its Guidelines for processing personal data across borders
- Your clients will increasingly require this information moving forward.

Bill 64:

- Transfers subject to verification of "adequate" protection

Implementation:

- Determine criteria for assessing the sensitivity of information, the purpose for its use and protective measures
- Establish "suitability" criteria
- Country risk assessment
- Adopt a service provider engagement policy accordingly

2.3. De-identification and anonymisation

- Criteria:
  - De-identification:
    - Replace identifiers with a hash
    - Limited use
  - Anonymisation:
    - Irreversible separation of identifiers
    - Use for serious and legitimate reasons
- Adopt reliable technologies
- Supervise internal use
- Define serious and legitimate reasons
- Develop public documents about practices

2.4 Mechanisms for responding to individual rights

Establish procedures to comply with:

- Right of access to the reasons for a decision based exclusively on automated processing
- Right to be forgotten
- Right to portability

Guidelines on the information to be made accessible:

- Procedure for an individual to “comment” the decision
- Guidelines to account for considerations of prejudice, public interest, legality
- Guidelines on the disclosure of information that has been "Created or Derived"

To summarize – 5 lessons learned from the review of internal compliance programs

What we have learned from studying our clients' compliance procedures:

1. “There is no point in running, you have to start on time”
2. Designation of a Data Privacy Officer (DPO) is a critical decision and options are varied
3. Planning of the compliance exercise should be based on a gap analysis and a risk analysis for every gap
4. Allocation of resources must be proportional to the effort
5. Compliance must be supported by a culture of PI across the organization

Upcoming related webinars:

- *Privacy regulation of de-identifcation and anonymsation is a game-changer – How to make it work in practice – Dr Khaled El-Emam*, November 4, 2021

- *Les recours des entreprises en vertu de la Loi 64 sur la protection des renseignements personnels – Comment vous protéger et comment vous défendre* (offered in French), November 2021

大成 DENTONS

Thank you

Chantal Bernier
National Practice Leader, Privacy and Cybersecurity, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Alexandra Quigley
Senior Associate, Montréal
D +1 514 878 5856
alexandra.quigley@dentons.com