CFIQ CONSEIL DES FONDS D'INVESTISSEMENT DU QUÉBEC

La voix au Québec de l'Institut des fonds d'investissement du Canada

IFIC.CA

JOHANNE BLANCHARD
Chair of the Board of Governors

August 31, 2020

BY EMAIL

The Honourable Simon Jolin-Barrette
Minister of Justice
Minister Responsible for the French Language
Minister Responsible for Laicity and Parliamentary Reform
Minister responsible for Access to Information and the Protection of Personal Information
Minister Responsible for the Montérégie Region
Government House Leader
ministre@justice.gouv.qc.ca

Committee on Institutions
Assemblée nationale du Québec
CI@assnat.qc.ca

Subject: CFIQ comments on Bill 64 – Protection of Personal Information

Dear Minister:

The Conseil des fonds d'investissement du Québec (CFIQ) presents its comments on *Bill 64, An Act to modernize legislative provisions as regards the protection of personal information* (Bill 64).

The CFIQ is the Québec voice of the Investment Funds Institute of Canada (IFIC), which is the voice of Canada's investment funds industry. IFIC brings together 150 organizations, including fund managers, distributors and industry service organizations, to foster a strong, stable investment sector where investors can realize their financial goals.

The CFIQ operates within a governance framework that gathers member contributions through working committees. The recommendations of the working committees are submitted to the committees of the CFIQ and IFIC and to the CFIQ board of governors. This process results in a submission that reflects the input and direction of a broad range of industry members.

Scope and structure of our comments

Our comments focus on the amendments to the *Act respecting the protection of personal information in the private sector (*Private Sector Act).

The structure of our comments is as follows:

I. General comments on Bill 64
II. Comments on the amendments to the Private Sector Act that are broader in scope
III. Comments on more technical issues of the proposed amendments to the Private Sector Act in Appendix 1.

I. General comments on Bill 64

We commend the Government of Québec for modernizing its privacy legislation. This issue is at the heart of a fair and efficient economy. The following are recommendations to further improve the objectives of Bill 64.

Coordinated modernization with other jurisdictions in Canada

Given that the governments of Canada, Alberta and British-Columbia also plan to modernize their privacy legislation in the near future, we recommend that the Government of Québec take a coordinated approach with the other jurisdictions to modernize its legislation. There will be significant time and compliance costs associated with the new requirements. It would not be reasonable, nor economically make sense for Quebec enterprises that operate across other jurisdictions, to comply with various legislations that have the same objective. A coordinated approach would reduce the regulatory burden on businesses operating in Québec, which would increase their efficiency, make them more competitive and reduce the prices of goods and services for Quebeckers.

We have also identified opportunities for harmonization with other jurisdictions in our comments.

> ***Recommendation: the government of Quebec and the other jurisdictions in Canada that are modernizing their privacy legislation should coordinate their activities so that businesses that operate across multiple jurisdictions have a single transition to go through.***

Improve the privacy regulatory system

It would be beneficial for the protection of the public and the efficiency of the private sector that privacy legislation be harmonized across Canada. As such, we recommend the creation of an umbrella organization for privacy regulators. The objective of this organization would be to harmonize regulation. Quebec, as well as other jurisdictions would keep their relevant competencies for privacy legislation and oversight.

A similar system that has worked well is the Canadian Securities Administrators[1] (CSA) that is an organization composed of the securities regulators of the ten provinces and three territories. The CSA is primarily responsible for developing a harmonized approach to securities regulation across the country. The Autorité des marchés financiers[2] (AMF), which is the regulator in Quebec for securities, is a member of the CSA.

Such a new regulatory system would maintain the highest standards of privacy protection for Quebeckers while reducing the regulatory burden for Quebec enterprises, which is an important element to help our enterprises be more competitive in a globalized economy.

> ***Recommendation: the establishment of an organization composed of the Commission d'accès à l'information and other privacy regulators in Canada to harmonize privacy legislation. This organization could be similar to the CSA.***

Structure of Bill 64

We believe that Bill 64 could have been easier to read and understand if it were better structured and with simpler language. A number of definitions are provided in the sections of the Bill. It would have been easier for the reader to have a separate section for definitions at the beginning of the Bill. We also find that the language used is technical and not accessible to everyone. Given that Bill 64 affects all businesses that collect personal information, we recommend that the requirements be presented in plain language, to make them easier to understand for managers of small and medium-sized businesses (SMEs), which do not have the same legal resources as big firms. This would improve compliance with the Private Sector Act, which would benefit all

[1] https://www.securities-administrators.ca/
[2] https://lautorite.qc.ca/grand-public

stakeholders.

Recommendations:

i. Put the definitions in a separate section at the beginning of the Bill

ii. ***Use plain language to improve the understanding of the Bill by stakeholders***

Need for definition or clarification

Bill 64 often incorporates terms or concepts that require further definition or clarification. We have identified these points in our comments.

Coming into force and implementation timetable

Many new requirements in Bill 64 require significant time and resources, including technology, to implement. Other measures that are not complex can be implemented more quickly. In addition, companies must be given the time they need to renew the consent agreements already obtained from the public in accordance with the new requirements. Therefore, we recommend that Bill 64 take into account the complexity of the new requirements and adjust the transition periods accordingly. This would result in staggered effective dates and would allow for a viable transition for Québec businesses.

In addition, Bill 64 provides for the publication of regulations and guides to clarify certain clauses. We recommend that these regulations and guides be published for consultation before the final amendments to the Private Sector Act.

Recommendations:

i. Introduce transition periods that take into account the complexity of the changes that are required

ii. Regulations and guidelines should be published for consultation before the final amendments to the Private Sector Act

II. Comments on the broader amendments to the Private Sector Act

Assessment of privacy-related factors (Section 3.3)

The current wording of this section requires businesses to conduct an assessment of privacy-related factors for any project or system involving personal information. The industry is of the view that only high-privacy-risk projects require such an assessment, an approach that would be consistent with other privacy law regimes such as the European Union's General Data Protection Regulation (GDPR). These assessments require considerable financial, human and technological resources. In order for private sector projects to be economically viable, we recommend incorporating the notion of sensitivity of information with respect to its intended use when imposing such an obligation on private sector enterprises. The notion of sensitivity in this case could be based on the definition in section 12 of the Private Sector Act, as a prerequisite for an assessment of privacy-related factors.

Furthermore, Bill 64 is silent on what elements should constitute an assessment of privacy-related factors. Section 3.3 should provide specific guidance on what should be included in an assessment of privacy-related factors. These criteria should be harmonized with those of other privacy regimes. As many businesses operating in Québec also operate elsewhere, it could be a substantial burden if a business were required to complete multiple assessments that vary across jurisdictions.

Recommendations:

i. Incorporate into section 3.3 the notion of sensitivity of information with respect to its intended use, as defined in section 12 of the Private Sector Act, as a prerequisite for an assessment of privacy-related factors.

ii. Specify the criteria that private sector businesses must meet to meet the requirement to conduct an assessment of privacy-related factors. These criteria should be harmonized with other privacy regimes.

Consent requirement (Section 14)

The first paragraph of section 14 requires that consent be "… clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language and separately from any other information provided to the person concerned."

The industry is concerned with the proposed requirements for consent given that obtaining specific and detailed consent for each use of data that may be involved in the provision of a product or service will be virtually impossible to operationalize, especially for larger firms. The provision of personal data occurs at practically every level of commercial activity and requiring express consent for each use of information is simply not reasonable. Large companies may have hundreds of service providers across multiple jurisdictions, making requirements for disclosure and obtaining express consent impractical, if not impossible. Requiring consent for each specific purpose will overwhelm clients as well.

A Supreme Court of Canada (SCC) decision in 2016[3] confirmed that when organizations make the determination of an express or implied consent, they need to take into account the sensitivity of the information and the reasonable expectations of the individual, both of which will depend on context. Hence, express consent should only be used for circumstances involving sensitive information. This principle is also recognized in section 13 : " Such consent must be given expressly when it concerns sensitive personal information." The proposed consent requirements in section 14 introduce regulatory misalignment with section 13, the SCC decision and the federal, provincial and other international privacy regulations.

In addition, there is a need to define what is meant by "separately from any other information provided to the person concerned."

Recommendations:

i. There should not be a requirement for obtaining specific and detailed consent for each use of data that may be involved in the provision of a product or service.

ii. Express consent should be necessary only when an information is sensitive. This would also align section 14 with section 13.

iii. Define what is meant by "separately from any other information provided to the person concerned."

Communicating information outside Québec (Section 17)

Section 17 provides that information may be communicated outside Québec if an assessment of privacy-related factors "… establishes that it would receive protection equivalent to that afforded under this Act." Contractual clauses on privacy-related factors can establish protection equivalent to that afforded under this Act. We recommend that the Private Sector Act explicitly recognize

[3] *Royal Bank of Canada v. Trang*, 2016 SCC 50 § 23: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16242/index.do

contractual clauses as equivalent protection. PIPEDA[4] and GDPR[5] explicitly allow for this type of alternative.

Recommendation: We recommend that section 17 explicitly recognize contractual clauses as an equivalent protection to the Quebec legislation.

List of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec (Section 17.1)

We recommend that the list of jurisdictions whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec (list of equivalent jurisdictions) be published on the same date as the final amendments to the Private Sector Act. In addition, given that the other provinces and territories in Canada are major economic partners of Quebec, we recommend that the list be clear about which jurisdictions in Canada are equivalent to that of Quebec. Failure to do so, could create confusion regarding acceptable jurisdictions and result in increased costs or disruption for businesses that transfer personal information outside Québec in the ordinary course for storage or processing.

We also understand that enterprises that transfer information to entities that are within the jurisdictions that are on the list provided by the Quebec government, do not need to establish protection equivalency. An explicit mention in this regard in section 17.1 would be helpful.

Moreover, it is not necessarily easy to find and consult the *Gazette officielle du Québec*. We recommend that this list also be accessible on the website of the *Commission d'accès à l'information* (CAI).

Recommendations:

i. ***That the list of equivalent jurisdictions be published on the same date as the final amendments to the Private Sector Act. The list should include the status of the equivalent jurisdictions in Canada.***
ii. ***Explicitly mention that enterprises that transfer information to entities that are within the list of equivalent jurisdictions do not need to establish protection equivalency.***
iii. ***That the list of equivalent jurisdictions also be accessible on the website of the CAI.***

Retention period and anonymization of information (Section 23)

Information retention period

Section 23 states that: "Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy or anonymize the information, subject to any preservation period provided for by an Act." There may be circumstances where the data must be retained for longer periods than prescribed by law, for example in cases of litigation or investigation.

[4] https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf , paragraphe (2) (c), section 23, Division 4, Part I (p. 33)
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, paragraphe 3, article 46 (p. 62)

Recommendation: We recommend adding a clause that would be harmonized with section 8 of Division I of Part I of PIPEDA[6]:

"(8) Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have."

Anonymization of information

We would like to emphasize that technologies that allow for the anonymization of personal information are not common. This situation is all the more problematic for SMEs that may not have the resources to develop internal solutions. The Québec legislature must provide for an adequate transition period after the publication of the final amendments to the Private Sector Act for technological solutions to be developed, tested and implemented. We recommend a two-year transition period.

Recommendation: We recommend a two-year transition period for anonymization requirements from the date of publication of the final amendments to the Private Sector Act so that businesses can have adequate time to implement technological solutions.

In addition, the last paragraph of section 23 requires that: "Information anonymized under this Act must be anonymized according to generally accepted best practices."

Recommendation: Clarification is required as to what the legislator means by "generally accepted best practices."

Monetary administrative penalties (Sections 90.1 to 92.2)

In a submission[7] to the Minister of Innovation, Science and Economic Development Canada in November 2019, as part of a consultation to modernize the PIPEDA, IFIC highlighted that non-compliance is often the result of a lack of clarity or certainty as to an organization's obligations under the Act. As such, privacy regulators should enhance the education, tools and resources available to organizations. In line with IFIC's recommendation, we urge the CAI to also enhance education and tools to all stakeholders in Quebec to improve compliance.

Second, as noted before, other jurisdictions in Canada are also modernizing their privacy legislation and may adopt similar financial penalties. It would be unfair for an enterprise operating in several jurisdictions in Canada to pay multiple penalties for the same incident. The financial penalties that are proposed are severe and if multiplied, could put at risk the viability of the enterprise. The objectives of financial sanctions are mainly to serve as deterrent to non-compliance and to penalize those who do not comply with the rules. The objective is not to financially harm an enterprise in a way that could be detrimental to its survival. We therefore urge the Quebec government to coordinate financial penalties with other privacy regulators in Canada, to ensure that the financial penalties that an enterprise would be subject to under the Private Sector Act are the maximum penalties an enterprise will pay in Canada. The CSA operates in this manner, where the principal regulator of a registrant takes charge in cases of non-compliance and if necessary, imposes a penalty. Under the GDPR, financial penalties are imposed by the principal regulator of the enterprise. Penalties are not multiplied if the enterprise operates in other jurisdictions within the European Union. We should have similar safeguards in Quebec and the rest of Canada. This point reinforces our previous proposal for greater coordination and harmonization.

---

[6] https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf </867 p. 22
[7] https://www.ific.ca/wp-content/uploads/2019/11/IFIC-Submission-Proposals-to-Modernize-PIPEDA-November-4-2019.pdf/23563/ (p.4 "Enhancing the Commissioner's Powers")

Lastly, section 90.2 states that "The Commission shall develop and make public a general framework for the application of monetary administrative penalties ...". We recommend that the general framework be published before the final amendments to the Private Sector Act for consultation.

Recommendations:

i. The CAI should enhance education, tools and resources for all stakeholders in Quebec to improve compliance.

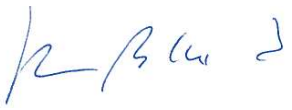
ii. The Quebec government should coordinate with other privacy regulators in Canada to ensure that any financial penalties imposed under the Private Sector Act are the maximum that the enterprise will pay in Canada.

iii. It is essential that the general framework for the application of monetary administrative penalties be published before the publication of the final amendments to the Private Sector Act for consultation.

* * * * *

We invite you to consult Appendix 1 for important comments on more technical issues. If more information is required, do not hesitate to contact Kia Rassekh, Regional Director of the CFIQ, by email at krassekh@ific.ca or by telephone at 514.985.7025.

Sincerely,



Johanne Blanchard
Chair of the Board of Governors
CFIQ

Appendix 1: Comments and recommendations on more technical issues

Third-party responsibility for retention (Section 1)

The industry supports the proposal that there is a responsibility to protect personal information "whether the enterprise keeps the information itself or through the agency of a third person."

Person in charge of the protection of personal information (Section 3.1)

The industry is in favour of the proposal that the person with the highest authority within an enterprise be, by default, the person in charge of the protection of personal information, with the possibility of delegation. This sends a clear message that the protection of personal information is an important issue at the highest levels and encourages a culture of sensitivity and compliance across the organization. In addition, the ability to delegate this function gives firms the necessary flexibility, because the person with the highest authority is not always the one with the required skills or the time to perform this important function.

Duty of transparency (Section 3.2)

The industry welcomes the duty of transparency to better inform the public about corporate policies for the protection of personal information. Since the policies of some firms could be complex and voluminous, we understand that the legislator is not asking that firms publish all of their policies in this area, but only an outline of these policies, so that stakeholders can better understand them and make an informed decision. To this end, we refer to the Government of Canada's PIPEDA[8] transparency requirements.

> ***Recommendation: that section 3.2 be aligned with PIPEDA's transparency requirements and that it specify that businesses are required to publish only an outline of their policies for the protection of personal information.***

Confidentiality incidents (Section 3.5)

In the event of a confidentiality incident involving personal information, this section requires the firm to notify "… any person whose personal information is concerned by the incident, failing which the Commission may order him to do so." We understand that, through this section, the Private Sector Act wants to give the Commission powers to order firms to comply with the requirement to report confidentiality incidents. However, we feel that the place chosen to do so is not appropriate. The words "...failing which the Commission may order him to do so" could suggest that the duty to report an incident is optional, unless compelled by the Commission to do so.

> ***Recommendations:***
>
> ***i. That section 3.5 be reworded to specify that an enterprise has an obligation to report a confidentiality incident without intervention by the Commission.***
>
> *ii.* ***The order-making power that the Private Sector Act wants to give the Commission should be provided for in a more appropriate section of the Act, possibly section 81.3, or through a regulation.***

In addition, the last paragraph of section 3.5 states: "A government regulation may determine the content and terms of the notices provided for in this section." We recommend that the government hold consultations on this regulation.

---

[8] https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf </878 ; sections 4.8, 4.8.1, 4.8.2, 4.8.3; pp. 54 and 55.

Recommendation: that the government hold consultations on the regulation to determine the content and terms of the notices under section 3.5.

Consent of minors (Section 4.1)

This section states that "The personal information concerning a minor under 14 years of age may not be collected from him without the consent of the person having parental authority, unless collecting the information is clearly for the minor's benefit." In the latter case, section 4.1 would, in our view, require clarification as to whether consent in such a situation can be sought directly from the minor or whether the business can proceed without the consent of the minor when collecting the information is "clearly for the minor's benefit." Furthermore, the notion of "clearly for the minor's benefit" could be subject to various interpretations, so clarification of this notion is necessary.

In addition, section 4.1 is not consistent with the second paragraph of section 14, which presents a more restrictive consent situation: "The consent of a minor under 14 years of age is given by the person having parental authority." The notion of "clearly for the minor's benefit" does not appear in section 14. This requirement difference can create confusion for businesses in implementing the Private Sector Act.

Recommendations:

i. ***Where collecting the information is "clearly for the minor's benefit," specify whether consent can be sought directly from the minor or whether the business can proceed without the minor's consent.***
ii. ***Section 4.1 must define the notion of "clearly for the minor's benefit."***
iii. ***The Private Sector Act must harmonize the consent requirements for minors under 14 years of age raised in sections 4.1 and 14.***

Requirements related to the collection of information using technology that allows for identification, locating or profiling (Section 8.1)

Recommendation: Clarification is needed as to whether the functions allowing a person concerned to be identified, located or profiled include cookies, which are commonly used on company websites.

Requirements related to the provision of a technological product or service (Section 9.1)

Recommendation: Clarification is needed to better define what is meant by "a technological product or service" and "…provide the highest level of confidentiality …"

Collection without consent, de-identification and anonymization (Section 12)

This section provides that personal information may be used for a purpose other than that for which it was collected, without the consent of the person concerned, only in the following cases:

(1) If it is used for purposes consistent with the purposes for which it was collected;

(2) If it is clearly used for the benefit of the person concerned;

Recommendation – There is a need to define and provide specific examples of what is meant by "for purposes consistent with the purposes for which it was collected" and "it is clearly used for the benefit of the person concerned."

In addition, this section defines "de-identified" personal information. Section 23 defines "anonymized" personal information. It is important for businesses to understand the difference between these two types of information and to have specific examples of how each of these methods can be used in a business.

Recommendation: Explain in practical terms the difference between "de-identified" and "anonymized" information with specific examples.

Consistent with the privacy legislation of Alberta and British Columbia, section 12 should exempt from the consent requirement the collection, use and disclosure of employee personal information that is necessary for establishing, managing or terminating an employment relationship. Given the requirement in section 14 that consent be "free", the absence of an exemption for employee personal information could result in situations where such information simply could not be collected, used or disclosed, as there may be hurdles to substantiating that an employee's consent was "free".

Recommendation: Include an exemption from the requirement to obtain consent in the context of employee personal information that is necessary for establishing, managing or terminating an employment relationship.

Communication for the purpose of concluding a commercial transaction (Section 18.4)

We applaud the inclusion of this section, which takes into account the needs and realities of B2B transactions. In the investment fund industry, this will facilitate the sharing of information during negotiations for the sale of clients between financial services representatives.

Non-adversarial inquiries (Section 83)

We understand that non-adversarial inquiries are collaborative.