November 4, 2019

Delivered By Email

Mr. Charles Taillefer
Director, Privacy and Data Protection Policy Directorate
Digital Policy Branch
Innovation,Science and Economic Development Canada
charles.taillefer@canada.ca

Dear Mr. Taillefer:

RE: Proposals to Modernize the *Personal Information Protection and Electronic Documents Act*

The Investment Funds Institute of Canada (IFIC) appreciates the opportunity to comment on the proposals to modernize the *Personal Information Protection and Electronic Documents Act* (**PIPEDA** or the **Act**).

IFIC 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. IFIC works collaboratively with industry representatives, regulators, governments and investor advocates to help cultivate a system that is fair, secure and efficient for all stakeholders.

IFIC operates on a governance framework that gathers member input through working committees. The recommendations of the working committees are submitted to the IFIC Board or board level committee for direction and approval. This process results in a submission that reflects the input and direction of IFIC members.

IFIC agrees that individuals should have meaningful control over their personal information and their privacy. We are encouraged that, in addition to considering a plain language rewrite of the Act, the proposals intend to support innovation and facilitate an integrated digital economy at both the domestic and international level. To help facilitate these objectives, our members agree that it is necessary to take steps to modernize PIPEDA.

The proposals raise many thoughtful considerations and questions. Our submission does not respond to all of the questions posed, but focuses on key considerations relevant to the investment funds industry.

Prohibiting the Bundling of Consent into a Contract

The proposal requires additional clarity as to what "prohibiting the bundling of consent into a contract" intends to forbid. In reviewing various regulations, it appears that bundled consent can either refer to a variety of terms and conditions that are bundled together into a single consent or a single consent that applies to a range of collections, uses and disclosures specific to personal information.

Prohibiting the bundling of consent into a contract should be specifically defined so that the practical implications can be properly evaluated.

Standard Business Activities

IFIC commends the Office of the Privacy Commissioner of Canada (OPC) for concluding its consultation on transfers for processing quickly and providing organizations with certainty. We appreciate the practical approach the OPC has taken by maintaining the status quo until the law is changed.

While the current non-legal drafting of PIPEDA may not reflect the desired form and substance, it has resulted in a flexible, pragmatic approach to its interpretation and application. Any proposal to modernize PIPEDA should continue to facilitate a practical approach to privacy and the application of the rules.

The introduction of a definition of standard business activities that do not require consent as set out in the proposal, is a more practical way to address this flow of information. As described in our submission to the OPC[1], the investment funds industry requires the constant flow of information between investment fund manufacturers, distributors and service providers. Requiring consent for the transfer of personal information would result in significant, if not insurmountable, operational challenges with little or no corresponding benefit to investors. Standard business activities, including transfers for processing, are more appropriately addressed contractually between the organization and the third party processor. The terms of any such contract should reinforce appropriate controls and help underscore the accountability of the collecting organization to retain control of the information.

The definition of standard business activities should include, but may not be limited to, the following range of activities:

- transfers to affiliated or third party service providers responsible for processing or handling the personal information of consumers or employees on behalf of the recipient of the personal information
- software and data storage providers
- responding to valid and authorized information requests from domestic and international authorities
- as permitted or required by law, to comply with laws, regulations, subpoena or court order
- for the purposes of fraud or crime prevention, suppression or detection
- to protect the personal safety of employees, clients or other third parties

Although some of the above noted activities may be covered in other areas of the Act or the accompanying guidelines today, a robust and inclusive definition of standard business activities will help provide organizations with clear information in one location.

Sensitive Personal Information

The current contextual approach to sensitive personal information may afford flexibility but may not provide enough information to help organizations comply with the rule. Therefore, we agree that sensitive personal information should be defined. To the extent that other jurisdictions have defined sensitive personal information, it would be beneficial to adopt a substantially similar definition. As an example, the Australian Privacy Principles Guidelines[2] defines sensitive personal information as a subset of personal information and includes without limitation:

- information or an opinion (that is also personal information) about an individual's
  - racial or ethnic origin
  - political opinions or associations

[1] Refer to IFIC Submission – Office of the Privacy Commissioner of Canada – Consultation on Transfers for Processing https://www.ific.ca/wp-content/uploads/2019/08/IFIC-Submission-Office-of-the-Privacy-Commissioner-of-Canada-Consultation-on-Transfers-for-Processing-August-6-2019.pdf/22924/

[2] See section B.138 of Australian Privacy Principles Guidelines https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/

  - trade union membership or associations
  - religious beliefs or affiliations
  - philosophical beliefs
  - sexual orientation or practices
  - criminal record
- health information about an individual
- genetic information (that is not otherwise health information)

Data Mobility

Data mobility has the potential to improve upon the investment funds industry's ability to deliver a streamlined client experience. As such, IFIC supports data mobility, provided an appropriate framework for data transfer can be established. Such a framework will be contingent on the development of a standardized application program interface (API) that enables information exchange between parties.

A standardized framework must consider the obligation of participants to transfer the data that an individual has provided versus the transfer of accurate data. Individuals must continue to be solely responsible for the accuracy of their data. Organizations should not be held responsible for transferring inaccurate data provided by an individual.

Only data that has been provided by the individual should be subject to data mobility requirements. Data that has been derived by an organization, an affiliate of the organization, or a third party using the data on behalf of the organization should not be subject to these requirements. Derived data belongs to the organization and therefore should not be considered part of the information that is owned by the individual.

Data mobility should not generally include information pertaining to a third party who has not consented to the transfer of their personal information, with some limited exceptions. In the context of financial services, any data that is required to be collected by law should be transferrable. In some instances, this will include information about an individual's spouse or dependents. It would also be appropriate to transfer the contact information for providers of professional services to an individual, such as an accountant or lawyer.

Online Reputation

IFIC supports the principles behind the concept of erasure and the "right to be forgotten" and agrees that this can be a useful tool for enhancing control and maintaining an individual's reputation. It is however critical that this concept does not conflict with existing regulatory requirements or prescribed legislation (such as anti-money laundering laws). The investment funds industry has very specific requirements with respect to the collection and retention of client data. As such, the introduction of an individual's "right to be forgotten" must continue to allow businesses to comply with other regulatory or legal requirements to which they are subject.

There is some concern that this concept could be abused by malicious actors to engage in fraudulent activity. To help mitigate such unintended consequences, it is prudent to consider reasonable and responsible traceability.

Record Retention

The current principles pertaining to record retention are sufficient. The rules governing data collection and retention must continue to defer to the laws and limitation periods that impact an organization. Any other approach may result in conflicting requirements and unnecessary regulatory burden.

Self-Regulation and Technical Standards

IFIC appreciates the use of a flexible, principles based privacy framework to balance meaningful privacy protection with the interoperability of jurisdictional privacy frameworks. Having said that, principles based

regulations frequently result in a need for additional information or tools to help organizations better understand and achieve the intended outcomes.

A self-certification mechanism for organizations to proactively demonstrate compliance with PIPEDA can be useful in achieving compliance. Such programs often result in a robust infrastructure to underpin the certification. Internal control certifications, similar to those used to support Sarbanes-Oxley, Volcker and anti-money laundering compliance, have proven to be valuable in the financial services industry.

Alternatively, optional certification programs and certification bodies, similar to the recently announced CyberSecure Canada[3] program, can also be effective. While not mandatory, a certification program can help support an organization's effort to comply with regulations and increase consumer confidence. Such discretionary certifications can often be tailored to the nature and size of an organization.

Enhancing the Commissioner's Powers

As noted in the proposal, non-compliance is often the result of a lack of clarity or certainty as to an organization's obligations under the Act. As such, the OPC should enhance the education, tools and resources available to organizations before bolstering its enforcement practices. Privacy, much like cybersecurity, is best addressed by industry stakeholders working together to achieve better outcomes for consumers.

If, after improving upon the tools and resources available to help facilitate compliance with PIPIEDA, additional enforcement tools are necessary to address egregious behaviour, a continuum of remedies that is proportionate to the severity of the offence should be considered. A range of statutory penalties based upon factors similar to those outlined in the Mutual Fund Dealers Association of Canada (MFDA) Sanctions Guidelines[4] should be contemplated.

The proposals states that there is concern that the current ombudsman model and enforcement framework may be outdated and may not incentivize compliance. If the renewed framework intends to incorporate administrative monetary penalties, it will be important to create separation between the individuals responsible for investigating offences and those responsible for determining the corresponding penalty to address any potential conflicts of interest.

* * * * *

IFIC is supportive of the concepts discussed in the proposals. Given many Canadian organizations operate in a global environment, the expectations and requirements found in privacy legislation internationally must be considered. Canadian businesses that operate globally have spent considerable resources to comply with existing international regulations. Organizations, and the individuals they interact with, would not be well served by novel or conflicting privacy regulation. As such, ongoing collaboration is critical to strike the right balance for all stakeholders.

We would be pleased to provide further information or answer any questions you may have. Please feel free to contact me by email at mupadhyaya@ific.ca or, by phone 416-309-2314.

Yours sincerely,

THE INVESTMENT FUNDS INSTITUTE OF CANADA

By: Minal Upadhyaya
Vice President, Policy and General Counsel

[3] See the CyberSecure Canada website for additional information https://www.ic.gc.ca/eic/site/137.nsf/eng/h_00000.html

[4] See MFDA Sanction Guidelines https://mfda.ca/enforcement/sanction-guidelines/