

From: [Perras, Timothy](#)
To: [EconomicFuture Committee](#)
Subject: Review of Personal Information Protection Act - Call for Submissions
Date: Friday, February 26, 2016 8:20:06 PM
Attachments: [image001.png](#)
[PIPA Submission.pdf](#)

Good evening,

To the Honourable Members of the Standing Committee on Alberta's Economic Future:

On behalf of ATB Financial, please see our submission attached regarding the review of the *Personal Information Protection Act*.

Please let me know if any clarification is required. Many thanks in advance for your consideration!

Kind regards,

Timothy Perras CIPM, CIPP/C | Privacy Compliance Manager
2100, 10020 - 100 Street, Edmonton T5J 0N3 | Transit 115
Office [REDACTED] | **Fax** 780 392 7200

ATB Financial™ SAVING | BORROWING | INVESTING | KNOW-HOW

If you have received this email in error, please let me know by return email so I can make sure it doesn't happen again. Because emails can contain confidential and privileged material, I'd ask for your help by deleting it and any attachments. Thanks!

We like to keep people up to date with information about new products and services at ATB or changes that could affect you. You can check out more about ATB and CASL [here](#).

If you would like to unsubscribe from our updates, please click [here](#).

1. Are the provisions of the Act regarding the collection, use and disclosure of information by trade unions appropriate? Please explain why or why not and provide suggestions.

We believe the provisions are appropriate.

2. Should PIPA include additional exceptions to consent that would permit other kinds of organizations (i.e., other than trade unions) to collect, use or disclose personal information of individuals for purposes of free expression without those individuals' consent? If so, which kinds of organizations and for what types of free expression purposes?

As a financial institution with a duty to protect clients and employees' confidential and often sensitive personal information, we do not advocate additional exceptions.

3. Are the exemptions to PIPA appropriate?

Current exemptions to PIPA seem appropriate.

4. Are the provisions dealing with forms of consent and the conditions attached to their use appropriate? Please explain why or why not and provide suggestions.

We believe they are appropriate as PIPA provides a reasonable balance and flexibility for organizations to collect consent, and options for individuals to provide consent as required.

5. Does PIPA adequately support individuals who are unable to provide consent for the collection, disclosure and use of their personal information? Please explain why or why not and provide suggestions.

While PIPA does support this (e.g. under sections 61(1)(e) and (g)), we believe it could be bolstered somewhat. For example, there might be a situation where an individual appears to be incapacitated in some way and at risk of financial fraud/elder abuse. To help protect clients and their financial well-being, the Legislature could expand upon discretion in PIPA for organizations to disclose information which is reasonably required to assist in the foregoing. The challenge is there might actually be a POA or guardian in place (i.e. the POA might be the issue). To help organizations navigate through these muddy waters, the committee could build in additional discretion for organizations who clearly want to act in their clients' best interests but may be unable to assist for fear of violating PIPA, or where the law is silent etc.

6. Are the exceptions to consent for the collection, use, and disclosure of personal information appropriate? Please explain why or why not and provide suggestions.

The exceptions appear appropriate.

7. Should the provisions of PIPA pertaining to disclosure without a warrant be changed? If so, what should be changed?

Overall the provisions are adequate. As an FI, we routinely receive requests from law enforcement agencies and may have to consider sections 20(f) or (m) in the course of determining whether the police may need to apply for a production order, or where disclosure without consent is reasonable/defensible under such circumstances. Therefore, we believe it will be useful for the legislature to provide further clarity and direction on what organizations should do when faced with such scenario. The clarity we anticipate under this section will be to outline what circumstances organizations may release personal information in their custody to the police or the law enforcement agencies without a warrant. 20(m) says we may disclose if it is reasonable for the purpose of an investigation. The status quo creates situations where an organization may feel it is unreasonable to disclose but the police may feel it is reasonable to disclose without a production order.

8. Should organizations be required to publish transparency reports on disclosures made without consent to public bodies and law enforcement agencies?

No, as we believe this may prejudice the investigation in some situations. It is best to leave the discretion regarding disclosure to law enforcement and the public body.

9. Are the processes for accessing records of personal information appropriate? Please explain why or why not and provide suggestions.

It would be great to further clarify section 6(3) which provides that an organization must make written information about its policies and practices available upon request. This section appears to be at odds with the essence of section 24 which provides an individual with the right to request access for their own personal information in an organization's custody or control. It would be nice to clarify if/when an organization would be required to disclose a policy to an individual. Most organizations consider the content of their policy to be internal/proprietary information and would rather not disclose the information if the policy is not public. Based on section 6(3), it appears an organization may make a request to receive the internal policies of another organization. We do not believe that is the intention of the legislature.

10. Are the provisions regarding fees for accessing records of personal information appropriate? Please explain why or why not and provide suggestions.

We believe fees for access requests i.e. ability to charge reasonable fees is practical. However, it may be prudent to consider removing section 32(1)(1.1) PIPA because it creates situations where an employee may request all of their personal information knowing there is no fee. The organization may spend a lot of hours and cost trying to pull records from multiple systems especially for employees that have been with the company for many years. Sometimes, the employee may not even need most of the information. Removing the clause that says we may not charge a fee strikes a fair balance. Under FOIP, a public body may charge a fee regarding request for employee records. We advocate same under PIPA to create a level playing field. Overall, PIPA already says the fee must be reasonable and it is subject to review by the OIPC.

11. Should PIPA provide a fee structure for access to personal information? Please explain why or why not and provide suggestions.

We believe organizations should set fees based on what is reasonable.

12. Are the exemption provisions for refusing access to an individual's own personal information appropriate? Please explain why or why not and provide suggestions.

The exemptions seem appropriate.

13. Are the provisions pertaining to personal employee information appropriate? Please explain why or why not and provide suggestions.

We believe they are appropriate as they provide a reasonable requirement for collection, use and safeguarding without an onerous structure regarding notification.

14. Are the provisions pertaining to employee references appropriate, or is more clarity needed about the information that may be disclosed in a reference? Please explain why or why not and provide suggestions.

We believe they are appropriate.

15. Are the processes set out in PIPA for retaining, destroying, and caring for personal information appropriate? Please explain why or why not and provide suggestions.

We believe the provisions are appropriate.

16. Is the level of transparency required of organizations using third-party service providers outside of Canada sufficient? Please explain why or why not and provide any suggestions for improvement.

We believe notification regarding an organization's use of out of Canada service providers is sufficient.

17. Are the provisions of PIPA regarding notification of a breach of privacy appropriate? Please explain why or why not and provide suggestions.

We believe the provisions overall are appropriate. However, it would be great to define "real risk of significant harm" to ensure organizations fully understand when the threshold of harm is met which triggers notification to the regulator and impacted individuals.

18. Should the Commissioner's powers be changed or expanded? Please explain why or why not and provide suggestions.

We believe the Commissioner has adequate authority to enforce the Act.

19. Are the sections pertaining to offences functioning as intended and are they strong enough to deter breaches and actions in contravention of the Act? Please explain why or why not and provide suggestions.

Yes, we believe they are functioning as a deterrent effect to ensure organizations are compliant.

20. Are the provisions in the Act regarding professional regulatory organizations appropriate? Please explain why or why not and provide suggestions.

We believe they are appropriate.

21. Is the application of the Act to non-profit organizations appropriate, or should all non-profit organizations be subject to PIPA in all of their activities? Please explain why or why not and provide suggestions.

We believe application regarding non-profit organizations is appropriate.

22. Do you have any other suggestions or comments regarding PIPA? Please comment on any topic relevant to PIPA not addressed by this discussion guide.

Since the last major revision of PIPA, service providers are increasingly internet or cloud based. In particular, cloud service providers may operate in several jurisdictions or have multiple data centres or backups in various countries, etc. The Legislature may want to consider updating PIPA with additional provisions on requirements for cloud providers.