Alberta Personal Information Protection Act- Consultation May 2024

Question 1

Are there specific amendments needed to harmonize PIPA with other jurisdictions to make it easier for businesses to operate in all jurisdictions?

Response

- Alignment with International Standards: Harmonizing PIPA with international privacy laws, such as the EU's General Data Protection Regulation (GDPR), could help businesses operate more seamlessly across jurisdictions.
- Anticipated Amendments: Considering anticipated changes to federal privacy laws like PIPEDA may also be beneficial for maintaining consistency and competitiveness for businesses across different regions.
- Regulatory Consistency: A consistent regulatory approach across Canada could reduce the complexity and cost of compliance for businesses, especially those operating in multiple provinces.

Question 2

Are there specific amendments to PIPA needed to modernize the Act for relevant businesses and organizations to conduct business in Alberta?

Response

- Amendments to ensure Alberta's PIPA aligns with federal changes to maintain its exemption status, which may be affected by Bill C-27.
- Modernization suggestions from the Information and Privacy Commissioner (IPC) of Alberta, reflecting changes in the CPPA and supporting robust assessment of new technologies.
- Adjustments to address the relationship between provincial private sector privacy laws and the federal PIPEDA, especially concerning data that crosses provincial or national borders.

Question 3

Should PIPA include a framework to regulate the design, development, and/or use of artificial intelligence systems within Alberta? If so, what should be included?

Response

- Establish clear legal authority for collecting and using personal information within AI systems, ensuring any data collection complies with privacy laws.
- Implement robust consent mechanisms where AI systems rely on personal data, ensuring consent is informed, explicit, and meaningful.
- Maintain transparency in AI operations, clearly communicating how data is used and the privacy risks involved.
- Create strong safeguards to protect privacy rights, including measures to secure personal and sensitive information.
- Limit the sharing of personal, sensitive, or confidential information, and ensure that sharing complies with all relevant laws.

- Align the PIPA framework with federal privacy laws and international standards to ensure consistency and avoid conflicts.
- Provide specific guidance for small businesses on the responsible use of AI, helping them navigate the complexities of AI.
- Take into account recommendations for AI regulation under PIPEDA reform, adapting them to the Alberta context where appropriate.

Question 4

Should all non-profit organizations be fully subject to PIPA for all their activities?

Response

Non-profit organizations in Alberta are not automatically subject to PIPA; it depends on the nature of their activities and whether those activities are considered commercial. However, non-profit organizations collect personal information and should be subject to PIPA regardless of if the activities are deemed commercial or not.

Question 5

Should PIPA apply to political parties?

Response

Political parties, like other organizations, should be expected to handle personal information responsibly and transparently, adhering to the provisions for consent and transparency as mandated by PIPA. This would ensure they are accountable for their data practices, which is crucial for maintaining public trust in the political process.

Question 6

Should provisions be added to PIPA to further protect potentially sensitive information? If so, for which information?

Response

Considering technological advancements and increasing data breaches, it might be beneficial to review and potentially enhance provisions related to:

- Digital data security to address new forms of cyber threats.
- The scope of information considered sensitive, possibly expanding it to include biometric data.
- Clearer guidelines on the destruction and anonymization of personal data to prevent unauthorized reconstruction or identification.

Question 7

Should provisions be added for biometric information?

Response

Biometric information is increasingly becoming an important part of discussions around privacy and data protection due to its sensitive nature and the unique identifiers it provides for individuals.

- Specific provisions regarding biometric information could include the following:

    - Clear guidelines for organizations on the permissible use of biometric data.
    - A framework for accountability and transparency in the handling of biometric information.
    - Provisions to address consent requirements, limitations on collection, and measures for secure storage and destruction of biometric data.

Question 8

Should provisions be added to enhance the protection of children's personal information?

Response

Due to the digital age, enhancing protections for children's personal information under PIPA is extremely important and could include:

- Establishing more rigorous consent requirements for the collection, use, and disclosure of children's personal information.
- Creating clearer guidelines for organizations on how to handle children's personal information responsibly.
- Providing educational resources for both organizations and the public about the importance of protecting children's personal data.
- Similar to the GDPR, processing the personal data of any child under 16 requires parental consent.

Question 9

Are the provisions in PIPA dealing with forms of consent and the conditions attached to their use appropriate?

Response

They are, but the following enhancements should be considered:

- Clearer guidelines for organizations on how to implement the different forms of consent in practice, ensuring individuals are fully informed and their consent is meaningful.
- Increased transparency requirements for organizations, possibly through mandatory privacy impact assessments, to demonstrate how consent is being managed and personal information is being protected.
- Enhanced public education efforts to increase awareness of personal information rights under PIPA, including the importance and implications of giving consent.

Question 10

Should individuals receive notice in plain language when organizations explain the purposes for which personal information is collected, used or disclosed?

Response

- Organizations should provide notices in plain language to ensure individuals fully understand the purposes for which their personal information is collected, used, or disclosed.
- Plain language notices support the principle of informed consent, allowing individuals to make educated decisions regarding their personal information.

- Adopting plain language in privacy notices is considered a best practice in privacy protection and is encouraged by privacy advocates and regulators alike.

Question 11

Should PIPA include other protections for individual information, such as an individual's right to be forgotten or de-indexed?

Response

The inclusion of a 'right to be forgotten' could provide individuals with greater control over their personal information, allowing them to request the deletion of their data under certain conditions.

However, organizations could face the following challenges in implanting this:

- Adapting existing information systems to accommodate the erasure of data upon request, which may require significant changes to data architecture and storage practices.
- Developing new processes and training staff to handle requests for data deletion, which could be resource-intensive and require ongoing attention.
- Addressing the impact on backup and archival systems, which are designed for data preservation and may not easily support selective erasure of information.

Organizations would need to weigh the costs and benefits, possibly looking at the experiences of entities in the EU under the GDPR as a case study for implementation strategies and best practices.

Question 12

Upon an individual’s request, should organizations be required to transfer that individual's digital personal information to another organization in a structured, commonly used, and machine-readable format when it is technically feasible (data portability)?

Response

Implementing data portability presents a range of challenges for organizations, but it also offers opportunities to empower consumers and stimulate competition and innovation in the digital economy.

Challenges include:

- Ensuring the technical infrastructure is in place to support data portability can be complex and costly.
- Establishing common standards for data formats and transfer protocols is essential but can be difficult to achieve across different systems and sectors.
- Protecting the data during transfer and ensuring that the receiving organization has adequate security measures in place is a significant concern.
- Organizations must navigate various legal frameworks and ensure compliance with data protection laws, which can vary by jurisdiction.
- Educating consumers about their rights and the processes involved in data portability is necessary to ensure its effective use.

Question 13

Should organizations be required to provide individuals with the logic involved in automated decision making about that individual (algorithmic transparency)?

Response

Implementing algorithmic transparency poses several challenges to organizations:

- Modern algorithms, especially those based on machine learning, can be incredibly complex and difficult for the layperson to understand.
- Organizations might resist revealing details that could compromise their competitive advantage or lead to intellectual property theft.
- Detailed disclosures may make AI systems more vulnerable to attacks, as hackers could exploit the transparency to find and target weaknesses.
- The process of making algorithms transparent can be costly, requiring additional resources to document, explain, and possibly redesign systems for clarity.
- There's a risk that in the process of making algorithms transparent, sensitive data could be exposed, violating individual privacy.

Question 14

Should PIPA regulate the de-identification and/or anonymization of personal information within the control of an organization and the subsequent use or disclosure of the de-identified or anonymized information? If so, how?

Response

Regulation could involve setting clear standards and guidelines for the de-identification process, ensuring that the risk of re-identification is minimized.

The following challenges however exist with regulating the de-identification and/or anonymization of personal information:

- Technological advancements that may make it easier to re-identify individuals from de-identified data.
- Ensuring compliance across various sectors with different types of sensitive information.
- The dynamic nature of data, where information considered non-identifying today may become identifying in the future due to new data linkages.
- Educating organizations about the importance of de-identification and the proper methods to achieve it.

Question 15

Should organizations be required to have a privacy management program and provide written information about the program to individuals and the Commissioner?

Response

Organizations should certainly have a privacy management program as it ensures accountability and compliance with privacy laws. The challenges in providing information about such programs to individuals and the Commissioner include ensuring that the information is comprehensive yet understandable, maintaining up-to-date records, and

safeguarding sensitive details while being transparent. It's a balance between protecting individual privacy, meeting legislative requirements, and managing administrative and technical aspects of the program.

Question 16

Should organizations be required to complete and submit a privacy impact assessment to the Commissioner for specific initiatives involving personal information?

Response

Organizations are not currently mandated to submit a Privacy Impact Assessment (PIA) to the Commissioner for every project involving personal information. However, it is required for custodians under the Health Information Act. The process can be challenging due to the detailed analysis needed to identify potential privacy risks and the consideration of measures to mitigate these risks. Additionally, the review process by the Office of the Information and Privacy Commissioner (OIPC) can take up to 12 months, which requires organizations to plan accordingly.

Question 17

Are the provisions for notification of breaches to the Commissioner and individuals under PIPA appropriate?

Response

The recent changes, effective April 1, 2024, aiming to streamline the process, allow for more efficient resolution of privacy breach files and reducing backlogs. However, there's always room for enhancement. For instance, increasing transparency around the criteria that determine what constitutes a 'real risk of significant harm' could provide clearer guidance for organizations. Additionally, establishing more specific timelines for notifications and creating a public breach registry could further strengthen the framework.

Question 18

Should PIPA include the ability of the Commissioner to levy administrative monetary penalties against an organization for certain contraventions of the Act?

Response

Incorporating administrative monetary penalties within PIPA could serve as a strong deterrent against privacy violations. However, challenges may include ensuring that penalties are proportionate to the severity of the contravention and maintaining fairness in the imposition of fines. Additionally, there could be concerns regarding the potential for these penalties to be viewed as punitive rather than corrective, which might affect public perception and trust in regulatory processes.