

Alberta's Public Sector Privacy and Access to Information Regime Overhaul

Ronak Shah, Soha Atiq

December 2, 2024

Introduction

On November 6, 2024, Alberta's government introduced legislation to modernize the province's access to information and public sector privacy regime. Specifically, Alberta's government is proposing to divide the existing *Freedom of Information and Protection of Privacy* (FOIP) Act¹ into two acts: the *Protection of Privacy Act*² ([Bill 33](#)) and the *Access to Information Act*³ ([Bill 34](#)).

The new bifurcated regime brings Alberta in line with other Canadian jurisdictions, which have all updated their legislations since the [November 2019 resolution](#) by Canadian data protection authorities that urged all provinces and territories to update their access and privacy legislation. Both bills incorporate stakeholder feedback and extensive reviews of the current FOIP regime, which were undertaken by the government between 2020 and 2024.

Key Takeaways

- Bill 33: The proposed *Protection of Privacy Act* enhances and builds on the FOIP privacy rules by:
 - emphasizing that public bodies embrace a *privacy by design* approach by requiring that they implement privacy management programs and undertake privacy impact assessments.
 - introducing mandatory breach reporting and some of the strictest penalties for the misuse of personal information – with penalties up to to \$200,000 for individuals and \$1million for organizations.
 - establishing clear rules for how public bodies can create and use data derived from personal information (e.g., “non-personal data”) while continuing to protect Albertan's privacy.
- Bill 34: The proposed *Access to Information Act* aims to improve transparency and access to information while streamlining the process to reduce the administrative burden faced by public bodies when faced with such requests for information. Amendments include extended response times, new discretionary exemptions for certain types of information requests, expanding cabinet confidentiality, and preventing a public body from making a request to access a record in the custody or control of another public body.
- If passed, these acts would mark the first major update to Alberta's access and public sector privacy

laws since the early 2000s, with further regulations and guidance expected in Spring 2025.

Bill 33 - Protection of Privacy Act (POPA)

POPA builds on existing privacy law requirements with a view to strengthen the rules that govern the protection of personal information held by public bodies by requiring them to focus more attention on their data management practices. POPA emphasizes the principles of accountability, transparency, data protection and data minimization. Outlined below are key highlights proposed under POPA:

- **Scope:** In addition to regulating how public bodies collect, use, and disclose personal information, it proposes to regulate their creation and processing of data derived from personal information such as “non-personal data.”
- **Privacy by Design:** POPA enhances privacy protections by requiring that public bodies adopt a “privacy by design” approach to their programs and services by mandating privacy assessments and privacy management programs. This means public bodies must consider the privacy implications of how they manage personal information when they do business and create or make changes to their programs, systems, or services.⁴
- **Mandatory Breach Notification:** Public bodies must notify impacted individuals, Alberta's Office of the Information and Privacy Commissioner (OIPC), and the Minister of Technology and Innovation without unreasonable delay if there is a loss of or unauthorized access to or disclosure of personal information under the control of the public body that poses a real risk of significant harm, such as identity theft or financial loss. The proposed notification threshold aligns with the mandatory breach notification requirements across Canada.
- **Privacy Management Programs:** Public bodies must develop and implement a comprehensive privacy management program, documenting their privacy practices and promoting compliance with the legislation. To prevent administrative burden to public bodies, the scale of the programs would be proportional to the volume and sensitivity of the personal information under control. Details of the public body's privacy management program must be made available to the public upon request.
- **Privacy Impact Assessments (PIA):** PIAs will be mandatory in certain prescribed circumstances that will be identified in forthcoming regulations.
- **Prohibition on Selling Personal Information:** Public bodies are explicitly prohibited from selling personal information under any circumstances, ensuring that data is not used for marketing or advertising purposes.
- **Data Matching to Create Data Derived from Personal Information:** Public bodies are permitted to carry out data matching – the linking of personal information from two or more databases or other electronic sources of information – to create ‘data derived from personal information’ for: (a) research and analysis; (b) program and service design, delivery and evaluation; or (c) any other prescribed purposes. For the purposes of data matching, public bodies cannot directly seek out personal information from individuals, but they may use databases containing personal information

that is under their control or collected by another Alberta public body. This could give public bodies the ability to take a data-centric and tailored approach to service and program delivery, and for greater cross-ministry collaboration. For example, two government ministries could align their datasets to assess eligibility for an applicant for a jointly delivered program. The public body must destroy data derived from personal information or transform it into non-personal data as soon as reasonably possible after it has finished using this data.

- **Non-Personal Data Usage:** POPA now imposes requirements on the use of ‘non-personal data.’ Currently, ‘non-personal data’ is broadly defined such that it would encompass: (a) de-identified data; (b) anonymized data; and (c) “synthetic data,” which is artificial data derived from real data (not defined) that has been de-identified. Public bodies must ensure that non-personal data is created for the following purposes: (a) research and analysis; (b) program and service design, delivery and evaluation; or (c) any other prescribed purposes. However, once created, POPA confusingly permits public bodies to use non-personal data for *any* purpose. Non-personal data must be created using generally accepted best practices or prescribed requirements. Additionally, public bodies must safeguard non-personal data and maintain robust records that document: source data, the purpose for which it was created, methods used to create it, and assessments undertaken to ensure that the non-personal data cannot be used to identify or re-identify a data subject. POPA imposes further requirements on the disclosure of non-personal data to persons other than a public body.
- **Enhanced Transparency:** For instance, public bodies must notify individuals if their personal information is used in an automated system to generate content or make decisions, recommendations, or predictions.
- **Enforcement:** POPA introduces some of the strictest public sector penalties in Canada for privacy violations, with penalties reaching up to \$200,000 for individuals and \$1 million for organizations. It also streamlines some of the administrative burden imposed on the OIPC. For example, it requires that a person first try to address the complaint with the public body prior to submitting one with the OIPC.

Bill 34 - Enhancements to the Access to Information Act (ATIO)

ATIO aims to improve transparency and access to information while addressing concerns resulting from the administrative burden that may arise from requests for access to public records.

Key changes under ATIO include:

- **Records Now Include “Electronic Records”:** In a nod to the ongoing digitization of government and the public sector, ATIO clarifies that a record includes “electronic records.” An “electronic record” is defined broadly to be a record that existed or is routinely generated at the time of request that is represented in a digital form that was created, maintained, archived, retrieved or distributed

Cassels

by computer systems.

- **Extended Response Times:** The time limit for responding to information requests is extended from 30 *calendar* days to 30 *business* days, with provisions for further extensions in certain circumstances. For example, it allows for extensions during times of emergencies so public bodies can focus on the immediate crisis.
- **Discretionary Exemptions:** ATIO empowers public bodies by providing some circumstances where they may disregard requests for information. For example, a public body may disregard requests if responding to it would unreasonably interfere with the operations of the public body or if the information has already been disclosed or made publicly available. However, in such circumstances the applicant must be provided reasons for the decision and the applicant may be able to ask the OIPC to review the decision.
- **Narrower Access to Government Deliberations:** Under ATIO, the scope of exemptions for cabinet and treasury board confidences is expanded, limiting access to sensitive government deliberations. Additionally, records of communication between political staff or a member of the Executive Council and political staff that does not involve any other employee of the public body fall outside ATIO's scope. These changes to the access regime could raise concerns about further government secrecy.
- **Protection of Workplace Investigative Records:** ATIA introduces exemptions for the disclosure of workplace investigations if their release could interfere with, prejudice or otherwise harm the investigation, a witness or a third party, or prevent witnesses from coming forward.

Conclusion and Next Steps

If passed, ATIO and POPA would mark the first major upgrade to Alberta's access and public sector privacy laws since the early 2000s. It may also foreshadow Alberta's approach to updating its private sector privacy regime. Alberta's *Personal Information Protection Act*⁵ which is currently undergoing a legislative review by the Standing Committee on Resource Stewardship, which began in January 2024. The Committee is expected to table its final report in June 2025.

If passed, both POPA and ATIO would come into effect upon proclamation, most likely sometime in Spring 2025. Additionally, the Alberta government has signalled that in Spring 2025 they will come forward with regulations and guidance for stakeholders, which will provide clarity on specific requirements such as those in relation to PIAs and privacy management programs.

¹ *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25.

² Bill 33, *Protection of Privacy Act*, 1st Session, 31st Leg, Alberta, 2024.

³ Bill 34, *Access to Information Act*, 1st Session, 31st Leg, Alberta, 2024.

⁴ Bill 33: Getting to know Alberta's proposed public sector privacy law. Available at: <<https://www.alberta.ca/system/files/bill-33-getting-to-know-protection-of-privacy-act.pdf>>.

This publication is a general summary of the law. It does not replace legal advice tailored to your specific circumstances.