Bill 33 Protection of Privacy Act

Getting to know Alberta's proposed public sector privacy law.

Alberta's government is proposing to repeal the *Freedom of Information and Protection of Privacy* (FOIP) *Act* and split it into two separate pieces of legislation – one dealing with protection of privacy and the other addressing access to information. Bill 33 *Protection of Privacy Act*, led by Technology and Innovation, will offer stronger privacy protections, maintain public trust, and improve government's ability to deliver services and programs. Bill 34 Access to Information Act, led by Service Alberta and Red Tape Reduction, will enhance access to information rights to align Alberta's practices with global best practices.

The existing FOIP Act applies to about 1,200 public bodies, like school districts, post-secondary institutions and municipalities, all of which will be affected by the legislative changes under the proposed new bills.

A public body is a government department, branch or office, an agency, board or commission, an educational body (like a school board or postsecondary institution), or a local government body (such as a municipal government, police service, library).

This fact sheet about Bill 33 Protection of Privacy Act provides a high-level summary of the changes public bodies will need to adopt and explains how Albertans will benefit from the proposed changes.

Times have changed, our laws must too

Alberta's privacy law is outdated and must be refreshed to meet the realities of the modern world. FOIP was introduced in 1995, and its last significant update was in the early 2000s. In this age of rapidly changing technology, people want assurance that their private information is protected. Technology like email, databases and artificial intelligence, that were more theoretical than reality when the FOIP Act was introduced, are increasingly integrated into daily life.

Feedback from Albertans

To ensure changes to privacy reflect the needs of public bodies, Alberta's government has been consulting with stakeholders since 2020. This included a public survey administered in 2021. Albertans said their privacy is a key priority and they have high expectations of public bodies in protecting their personal information. These extensive conversations highlighted the need for Alberta to address several items that are reflected in the bill.

Strongest privacy protections

Albertans should have confidence that their personal information is protected. Alberta's government is implementing the strongest privacy protections in Canada and the strictest penalties for violations.

The proposed Protection of Privacy Act enhances privacy protections by requiring that public bodies adopt a "privacy by design" approach to their programs and services. 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, services and systems.

Bill 33 builds on existing legislated protections of personal information by introducing some new rules:

- Public bodies cannot sell personal information in any circumstance or for any purpose, including marketing and advertising.
- Public bodies must notify Albertans if their information is used in an automated system to generate content or make decisions, recommendations, or predictions.
- Albertans must be notified about a privacy breach where there is a real risk of significant harm (e.g., bodily harm, financial loss, identify theft, fraud, blackmail). When Albertans are aware of a breach of their personal information, they can take actions to further protect themselves.

These changes are mandating global best practices that many Alberta public bodies already have in place.

Privacy Management Programs

Albertans are increasingly aware of their privacy rights and expect organizations to ensure personal information is secure and have protections against data breaches. This is why Alberta's government will make it mandatory for public bodies to adopt a privacy management program. Public bodies must document policies and procedures that outline their privacy practices, foster a culture of privacy, and promote compliance with legislation. Albertans will be able to request a copy of any public body's program.

For more information, visit www.alberta.ca/strengthening-the-protection-of-personal-information

Privacy Impact Assessments (PIAs)

PIAs are tools used to ensure programs and services comply with privacy legislation, identify and address privacy risks, and put in place safeguards to protect personal information. PIAs help organizations analyze how personally identifiable information is collected, used, shared, and maintained.

The proposed act will make PIAs mandatory for all Alberta public bodies in some circumstances. This new requirement is considered best practice and is already required under the *Health Information Act*.

New data rules

The proposed Protection of Privacy Act will improve public bodies' ability to deliver programs and services by including rules around data use. This means that the right information can be in the right place at the right time to ensure the best possible service delivery for Albertans.

Wherever possible, public bodies must use only the information that is absolutely necessary for research, analysis, or program and service design and delivery. They must use non-personal data, which is data with personally identifiable details like name or contact information removed. Personal information must be stripped so data no longer identifies a specific individual. Common uses for such de-identified data include analysis to identify trends (e.g., how many people from different demographics are using a service) or to improve the services provided. Public bodies are banned from selling data.

Bill 33 empowers public bodies to link personal information between sources under the control of different public bodies, a practice called data matching. For example, two government ministries aligning their datasets to assess program eligibility for an applicant.

Common sense changes

The proposed Protection of Privacy Act includes other, common-sense changes. For example:

- Public bodies will have clear rules for when and how to share information with each other to provide a common or integrated service, so Albertans don't have to repeatedly provide their information. For example, during emergencies, Albertans could be quickly assessed for eligibility for supports that are provided by various public bodies.
- Clarifying in collection notices that Albertans can contact public bodies by email not just by mail or phone. Also, that a collection notice does not need to be repeated if information is collected from the same person for the same reason.
- Requiring regular review of the Act.

Changes for the Office of the Information and Privacy Commissioner (OIPC)

Reducing administrative burden for the OIPC is important to ensure fair administrative procedures and to save time and resources. For example:

- A person must first try to address the complaint with the public body before submitting it to the OIPC.
- The OIPC will have discretion to not pursue an inquiry if it does not make sense to do so, such as when the matter is already settled.

The OIPC will have the ability to issue an order:

- related to the new data provisions and to ensure the OIPC can properly perform its regulatory functions. If a public body is using non-personal data outside of the allowed purposes, the OIPC can investigate and enforce compliance, and
- requiring a public body to provide a copy of their privacy impact assessments or privacy management program to the OPIC.

New penalties

The proposed *Protection of Privacy Act* has the strictest penalties in Canada that courts can impose for the misuse of Albertans' personal information and data. Penalties vary based on the offense and whether it was done by an organization or an individual.

Offenses	Individual	Organization
Personal information	Up to $125,000	Up to $750,000
Data and non-personal information	Up to $200,000	Up to $1 million

An example of personal information misuse by an individual is if an employee was to intentionally use a client's personal information to cause the client harm, or if a public body were to knowingly disclose personal information to another public body without authority. An example of misusing data is if a research partner who received non-personal data from a public body knowingly re-identified non-personal data.

Regulations with more details to come

In Spring 2025, regulations will come forward with more details, such as specific requirements for the privacy management and privacy impact assessment programs. Additional information and resources will also be shared at that time to help public bodies learn about and align with the new requirements.

For more information, visit www.alberta.ca/strengthening-the-protection-of-personal-information