

Getting to know the *Protection of Privacy Act*

The *Protection of Privacy Act* enhances public sector privacy rules.

In December 2024, Alberta's government passed legislation to repeal the *Freedom of Information and Protection of Privacy* (FOIP) Act and split it into two pieces of legislation – one dealing with protection of privacy and the other dealing with access to information. The acts and associated regulations came into force in June 2025.

The *Protection of Privacy Act*, led by Technology and Innovation, offers stronger privacy protections, maintains public trust, and improves public bodies' ability to deliver services and programs. The *Access to Information Act*, led by Service Alberta and Red Tape Reduction, enhances access to information rights to align Alberta's practices with global best practices.

The *Protection of Privacy Act* applies to about 1,200 public bodies, like school districts, post-secondary institutions, and municipalities.

This fact sheet provides a high-level summary of the *Protection of Privacy Act* and explains how Albertans' personal information is protected.

Albertans should have confidence that their personal information is protected. With the *Protection of Privacy Act*, Alberta's government has implemented the strongest privacy protections and the strictest penalties in Canada.

Strongest privacy protections

The *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.

The act also introduces 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, identity theft, fraud, blackmail). When Albertans are aware of a breach of their personal information, they can take actions to further protect themselves.

These changes mandate global best practices that many Alberta public bodies already had in place prior to the introduction of the legislation.

Privacy Management Programs

Albertans are increasingly aware of their privacy rights and expect organizations to ensure their personal information is secure and protected against data breaches. This is why Alberta's government made it mandatory for public bodies to establish and implement 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.

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 act makes PIAs mandatory for Alberta public bodies before they launch new programs or change existing ones that collect, use, or disclose personal information. This new requirement is considered best practice and is already required under the *Health Information Act*.

New data rules

The *Protection of Privacy Act* improves public bodies' ability to deliver programs and services by including rules around data use. Public bodies may create, use, and disclose non-personal data only for research, analysis, or program and service design and delivery purposes. Non-personal data means data that has

been altered to remove personally identifiable details like name or contact information. Common uses for such data include analysis to identify trends (e.g., how many people from different demographics are using a service) or to improve the services provided.

The act 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 align their datasets to assess program eligibility for an applicant. These activities are only permitted for specific purposes and public bodies.

‘Common sense’ changes

The *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 the right information can be in the right place at the right time to ensure the best possible service delivery for Albertans. For example, during emergencies, Albertans could be assessed quickly 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, and 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.

The Office of the Information and Privacy Commissioner (OIPC)

The OIPC continues to oversee public sector privacy under the new legislation, which clarifies some elements of the Commissioner’s role to empower public bodies to resolve issues. For example:

- A person must first try to address the complaint with the public body before submitting it to the OIPC.
- The OIPC now has 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 now also can 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 *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.

Protection of Privacy Regulations

Two regulations came into force to support the *Protection of Privacy Act* in June 2025. They set out detailed but practical expectations to help public bodies protect Albertans’ privacy, build public trust, and strengthen accountability.

For more information about the regulations supporting the *Protection of Privacy Act*, visit alberta.ca/protection-of-privacy-act.

