Getting to know the Protection of Privacy regulations

Understand your rights under Alberta's new public sector privacy law.

The *Protection of Privacy Act* went into effect in June 2025. It modernizes the province's public sector privacy laws by introducing the strongest protections and strictest penalties to protect Albertans and their personal information.

Two new regulations that build on the Act also went into effect. The Act and regulations work together to provide detailed, practical guidance to help public bodies implement the new rules. The Protection of Privacy Regulation provides definitions for terms captured in the *Protection of Privacy Act* and the Protection of Privacy Ministerial Regulation provides specific requirements for concepts captured in the Act, like the privacy management program and privacy impact assessments.

This document provides information about the new requirements outlined in the regulations and how they support a higher standard of privacy for Albertans.

The Act defines a public body as:

- 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, or library.

Privacy Management Programs

Public bodies are required to establish a privacy management program that includes documented policies and procedures to address duties under the act that is proportionate to the sensitivity and volume of the personal information the body holds.

Privacy management programs must also include:

- designation or identification of a privacy officer,
- mandatory staff training,
- establishment of a security classification system,
- information about how breaches are managed,
- information about how complaints are handled, and
- timelines for periodic review, assessment and update of their privacy management program.

Public bodies must provide a copy of their privacy management program to anyone who requests it or make it publicly available. Specific contents of the program may not be available to not compromise security.

Breach management

A public body must notify an individual if their personal information is involved in a privacy breach with a real risk of significant harm such as identity theft or financial loss. The public body must also notify the Office of the Information and Privacy Commissioner and the Minister of Technology and Innovation.

The notification must explain what happened, what information was involved, and how the breach is being managed.

Privacy Impact Assessments

Public bodies are now required to complete a privacy impact assessment before launching new programs or changing existing programs that collect, use, or disclose personal information. The assessment must:

- describe the project,
- identify any risks to privacy, and
- explain how risks will be managed.

Privacy impact assessments must be submitted to the Office of the Information and Privacy Commissioner under certain circumstances, like when two or more public bodies share data with each other.

Data Matching

New rules for data matching limit its use to research, planning, and service delivery. Data matching is the practice of linking personal information between two or more sources under the control of different public bodies.

Strict security measures must be applied to the resulting data, and data must be destroyed once it is no longer needed. Data created through data sharing can only be shared when specific conditions are met.

Creating and Sharing Non-Personal Data

New rules are in place for creating and sharing non-personal data, which is information with personally

For more information, visit alberta.ca/protection-of-privacy-act

Alberta

identifying details removed so individuals cannot be identified.

Non-personal data can be shared between public bodies for research and planning, but strict safeguards must be in place to prevent reidentification.

Public bodies must keep records explaining how non-personal data was created. They must also ensure external parties receiving the data sign an agreement outlining use restrictions and requirements for destruction.

Definitions

New definitions for key terms help public bodies determine whether they have reasonable grounds to take a particular action or appropriate safeguards in place to protect the different kinds of data they hold.

Collection

Public bodies must clearly identify the following in the collection notice when using and disclosing personal information:

- what personal information the consent relates to,
- how it will be used or whom it may be disclosed to,
- how long consent lasts.

Extra care must be taken when obtaining consent from youth to ensure they understand what they are agreeing to.

POPA also allows public bodies to use personal information in specific circumstances, including if the individual consents to the information being used for a purpose other than why it was collected.

Other changes

Other changes resulting from the regulations include:

- Public bodies must apply reasonable security arrangements, including physical, technical, and administrative safeguards based on the sensitivity of the personal information or non-personal data they hold.
- Public bodies must regularly log system activity, conduct security assessments, and train employees on data protection.
- Special considerations apply when using artificial intelligence or other automated systems involving personal information.

For more information, visit alberta.ca/protection-of-privacy-act