Frequently asked questions:

# Bill 33 Protection of Privacy Act

## Why is this happening now?

Albertans value their privacy and the protection of personal information. As they rely more and more on technology in their day-to-day lives, Alberta's government is looking at how its legislation should continue to protect Albertans' privacy and reflect the new realities of an age of rapidly changing technology. Alberta's privacy laws are outdated and must be refreshed to meet the realities of the modern world.

The Freedom of Information and Protection of Privacy Act (FOIP) was introduced in 1995 and saw its last significant update in the early 2000s. Technologies like email, databases, and artificial intelligence that were more theoretical than reality when the Act was introduced are now regularly being integrated into our daily lives.

We have been engaging with stakeholders on matters relating to privacy since 2020. Those conversations identified that updates to privacy protections are critical and there is a need for several things, including:

- clear definitions and authorities within legislation,
- privacy management requirements,
- modern data management practices,
- improve Albertans' experiences with services and programs by enabling the ability to use information collected from Albertans between government programs and services,
- special protections for sensitive data, and
- improved timelines and regulatory processes related to the Office of the Information and Privacy Commissioner (OIPC).

Public bodies are expected to support the majority of amendments. They've been asking for updates to the legislation for years and proposed amendments address gaps public bodies have previously identified, such as the inclusion of privacy management requirements.

The OIPC has spoken at various forums recommending review and modernization of Alberta's privacy laws, including as part of a joint resolution in 2019 with Information and Privacy Commissioners and Ombudspersons from across Canada.

## What is a public body, as defined under the Act?

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, or library).

## What are the aims of Bill 33 Protection of Privacy Act?

The proposed Protection of Privacy Act enhances and builds on the protection of privacy rules that were in FOIP. The proposed legislation will:

- introduce enhanced privacy protections by adopting a privacy by design approach to programs and services delivered by public bodies, and
- introduce the strictest penalties in Canada for the misuse of Albertans' personal information.
- support more effective delivery of programs and services across public bodies by allowing for common and integrated programs.

We are also making common-sense updates to existing rules to streamline work and reduce red tape. For example, requiring a person who has a complaint to first attempt to resolve their complaint with the public body, before applying with the OIPC, and empowering the OIPC to disregard an inquiry where one is not required.

To ensure legislation is kept current, it must be reviewed within six years.

A few things are not changing. Under the new legislation public bodies will continue to:

- be mandated to manage and protect any personal information they hold or control, and
- have clear responsibilities to collect, use, and disclose personal information responsibly, ethically, and in accordance with the proposed Act.

## What do these changes mean for individual Albertans?

These changes mean Albertans can be confident that:

- public bodies cannot sell their personal information for any reason;
- privacy risks and actions to mitigate those risks are identified early and addressed in the development of programs and services;
- privacy breaches are taken seriously, and individuals are made aware if their personal information has been involved in a breach; and
- Public bodies have clear rules for when and how they share information.

## What are these stronger offences and penalties?

Bill 33 prohibits an individual from knowingly contravening sections, including:

- collecting, using or disclosing personal information without authority;
- attempting to re-identify an individual from non-personal data;
- making false statements to the OIPC;
- obstructing the OIPC; and
- failing to comply with an order issued by the OIPC.

We are also introducing new penalties and offenses for the misuse of data derived from personal information and non-personal data to ensure that public bodies are serious in their responsibility to protect Albertans' personal information.

Penalties vary based on the offence. Penalties can be up to $125,000 for an individual and $750,000 for an organization that knowingly contravenes Part 1 of

the Act, which relates to personal information. Penalties can be up to $200,000 for individuals and $1,000,000 for organizations that contravene Part 2 of the Act, which relates to data matching and non-personal data.

## What is privacy by design?

Privacy by design is an approach that considers how personal information is used and protected in every step of program and service design, delivery, and management. We intend to do this in a variety of ways:

- Privacy Management Programs will help Albertans understand how their personal information is managed by public bodies.
- Privacy Impact Assessments will assess and address risks during the development of new programs and services.
- Breach Reporting will ensure Albertans are aware if their personal information has been involved in a breach.

## Tell me about privacy management programs.

The proposed Protection of Privacy Act makes it mandatory for public bodies to have documented policies and procedures to outline privacy practices, foster a culture of privacy, and promote compliance with the legislation. Having policies and procedures ensures public bodies are properly equipped to manage and protect any personal information in their custody or under their control.

Individuals can request a copy of the program from the public body.

## Tell me about privacy impact assessments.

Privacy Impact Assessments are documents that outline the privacy risks associated with a program or service and the actions taken to protect personal information. While privacy impact assessments are currently mandatory under the *Health Information Act*, they are not mandatory under the *Freedom of Information and Protection of Privacy Act.*

Privacy impact assessments will be mandatory in specific circumstances for all public bodies. The regulations coming forward in Spring 2025 will provide further details on when these assessments will be required and what they must include.

The proposed Protection of Privacy Act provides the ability for the OIPC to request a copy of a program's privacy impact assessment.

## Who is affected by the new bill?

Public bodies in Alberta that are currently subject to the FOIP Act will be subject to the proposed Protection of Privacy Act. This includes, for example, government departments; provincial agencies, boards, and commissions; municipalities; school boards; police services; and universities and colleges.

All Albertans are affected by the proposed changes to Alberta's public sector privacy legislation.

## Do these changes affect private sector businesses?

No, the proposed Protection of Privacy Act will apply only to provincial public bodies operating in Alberta. Private sector entities in Alberta are subject to the *Personal Information Protection Act* (PIPA).

PIPA is undergoing a legislated review by the Standing Committee on Resource Stewardship, which started in January 2024. The Committee has 18 months to

complete its review and the final report is expected by June 2025. The committee's recommendations will inform Alberta's government in making future improvements to PIPA.

## When will changes take effect?

The proposed legislation will come into effect upon proclamation, in Spring 2025. The government is developing regulations to support the proposed Protection of Privacy Act, which will be introduced in the Spring sitting of the legislature. Other information to support public bodies, including tool kits, will be available when the legislation is enacted.

## What will be captured in the regulations?

Regulations are a form of legislative rules that provide additional information and direction related to a specific act. They are usually made by the Minister and approved by the Lieutenant Governor.

The regulations will provide more specific information, where required. For example, the regulations will provide more information around when a privacy impact assessment is required and what requirements it must meet.

These regulations will recognize the diversity of Alberta's public bodies to avoid significant increases in costs or workloads while still providing necessary protections. Requirements will be proportional to the size of the public body, the personal information within the public body, and the complexity of programs and services.

More information will be available about the regulations in the Spring.

## Will regulations give the Minister more power?

The pace of technology is constantly moving forward and we need a way for the Minister to update or clarify elements of the Act in regulations. The proposed Protection of Privacy Act will provide the Minister of Technology and Innovation with the ability to make regulations, which will streamline implementation of key privacy and data requirements, enable efficiency, and ensure requirements are current.

For example, the Minister will be able to introduce regulations as needed for:

- privacy management programs
- privacy impact assessments
- breach reporting
- data matching
- the creation, use and disclosure of non-personal data.

## Does the bill give the Information and Privacy Commissioner more powers?

The proposed Protection of Privacy Act will give the OIPC new powers that correspond with additions to the proposed legislation, including the ability to:

- request a copy of a public body's privacy management program;
- request a privacy impact assessment for a specific program or service.

The proposed Protection of Privacy Act gives the OIPC new powers to comment on the implications for protection of privacy related to data matching practices and the creation, use and disclosure of data derived from personal information and non-personal data. The OIPC will also be able to order public bodies to stop

activities related to data matching or data derived from personal information or non-personal data if the organization is operating in contravention of the Act.

The Act also allows the OIPC not to proceed with an investigation unless the applicant wants them to or if the OIPC deems it unnecessary.

These changes are informed by input from the OIPC and will help streamline operations and strengthen personal information protections for Albertans by holding public bodies to account.

## How do Alberta's current laws compare to the rest of the country?

Since 2019, every other jurisdiction in Canada has updated their FOIP Act equivalents in some capacity—in some cases, these updates have necessitated significant and transformative revisions as was seen in British Columbia and Manitoba.

Alberta's Protection of Privacy Act will have the strongest protections in the country and the strictest penalties.

| ***Jurisdiction*** | **Fine** |
|---|---|
| *British Columbia* | Individual: up to $50,000<br>Corporation: up to $500,000 |
| *Quebec* | Natural person: $5,000 - $100,000<br>All other cases: $15,000 - $150,000 |
| *Alberta* | *Personal Information*:<br>Individual: up to $125,000<br>Organization: up to $750,000<br><br>*Data matching and non-personal information*<br>Individual: up to $200,000<br>Organization: up to $1 million |

Note: British Columbia and Quebec have the next highest fines which is why they are used as comparators.

## How are Alberta's new protections the strongest in Canada?

The Protection of Privacy Act:

- Explicitly prohibits a public body from selling Albertans' personal information
- Mandates public bodies to have privacy management programs proportional to their organization to allow Albertans to understand how their personal information is being used and protected;
- Mandates privacy impact assessments to identify and mitigate risks, particularly in cases where there is sensitive or large amount of information;
- Requires privacy breach notifications to ensure individuals are aware if their information was breached;
- Establishes clear rules for how public bodies can create and use data created from personal information to protect Albertan's privacy.
- Alberta is the first jurisdiction in Canada to set these standards clearly in legislation.

## Will private sector laws be next?

It is important that Alberta's privacy laws reflect the needs of rapidly changing technology.

The *Personal Information Protection Act* is undergoing a legislated review by the Standing Committee on Resource Stewardship, which started in January 2024. The Committee has 18 months to complete its review and the final report is expected by June 2025. The committee's recommendations will inform Alberta's government in making future improvements to PIPA.

## Have you consulted public bodies about these changes?

Between 2020 and 2024, Alberta's government conducted extensive reviews and stakeholder engagements to understand where privacy laws could be improved. These engagements identified the need for clear definitions and authorities, inclusion of privacy management requirements, data management practices, and increased ability to use information collected from Albertans between programs and services, to name only a few takeaways. Input was collected from other provincial ministries, municipalities, postsecondary institutions, school boards, and the OIPC.

Albertans were invited to provide feedback in a 2021 public survey. The results clearly identified that privacy is a key priority for Albertans and that they have high expectations of public bodies in protecting their personal information.

Much of this feedback is addressed in the proposed legislation.

## What kind of support will be available to public bodies to ensure compliance?

We will inform stakeholders of the changes. We are working on guidance and interpretive materials to help public bodies understand new requirements and help them become compliant with the new legislation.

More information will follow in spring 2025.

## Can Albertans opt out of sharing their personal information?

No – public bodies need to collect certain pieces of information to deliver their services. For example, schools need to know the home address of students, as well as the names and phones numbers of guardians.

However, the proposed legislation will introduce new requirements for public bodies collecting information from Albertans, including notifying Albertans whether a program or services uses automated decision making. This keeps Albertans informed and aware of how their personal information is being used to provide services and programs.

## Can public bodies sell Albertans' personal information?

No. The government will never sell personal information or allow other public bodies to do so. The proposed Protection of Privacy Act expressly indicates that, "A public body is prohibited from selling personal information in any circumstances or for any purpose, including marketing and advertising purposes."

## Why does the bill include a new section on data derived from

Data holds incredible value for planning and delivering programs and services. Alberta's government is committed to protecting Albertans' personal information while making best use of our available data.

## personal information and non-personal data?

To accomplish this, the proposed legislation provides clear rules around data matching, as well as creating, using and disclosing non-personal data. This helps ensure that public bodies can use data appropriately and ethically to improve their services and programs, while respecting Albertans' privacy.

Public bodies can only disclose non-personal data to non-public bodies for specific purposes, such as for research, planning, or program/service evaluation, and with conditions to safeguard the data.

## What other changes are proposed that I need to know?

The proposed Protection of Privacy Act also addresses the need to modernize privacy legislation in Alberta, for example:

- Definitions for terms introduced in the updated sections of the legislation, including those outlined at the Definitions section of this document.
- Public bodies are accountable for informing people when they use personal information to decide that directly affects a person using an automated system,
- Notice must be given to the Information and Privacy Commissioner and any impacted individual, if there is a breach or loss of personal information that could result in significant harm, allowing the Commissioner to confirm whether appropriate action has been taken to address the breach.
- Individual Albertans will be able to request a review by the Information and Privacy Commissioner if they believe their personal information has been used in contravention of the Act for data matching or the creation of data derived from personal information or non-personal data.

## Definitions

## Bill 33 *Protection of Privacy Act*

The following are definitions from Bill 33 with examples to help understanding.

| | |
|---|---|
| Biometric information | Information derived from an individual's unique, measurable characteristics.<br><br>For example, fingerprints or iris scans. When an individual uses their thumbprint to unlock their phone, they are using their biometric information.<br><br>Biometric information is included in the definition of personal information and is unchanged from the original FOIP Act. |
| Common or integrated program or service | A program or service that is planned, administered, delivered, managed, monitored or evaluated by two or more public bodies, or a single public body on behalf of at least one other public body.<br><br>The 2023 Affordability Payments Program—which offered monthly payments for eligible Albertans and families—is an example of a common or integrated program. Several government departments worked together to make the program possible.<br><br>While this concept already existed under the FOIP Act, it was not defined. The update will help clarify when public bodies can share personal information that is directly needed for operating a common or integrated program or service. |
| Data matching | Linking personal information between two sources that are under the control of different public bodies. Appropriate security measures must be in place.<br><br>For example, two government ministries could align data sets to assess program eligibility. |
| Personal information | Recorded information about an identifiable individual.<br><br>This includes someone's name, address, race, marital status, biometric information, educational background and more. |
| Privacy impact assessment | Privacy impacts assessments are a tool used to ensure programs and services comply with privacy legislation, identify and address privacy risks, and put in place appropriate safeguards to protect personal information.<br><br>For example, a public body that wants to use new software for a service must be thoughtful and document how any personal information that is collected, used, disclosed, stored, and protected through a privacy impact assessment. |
| Privacy management program | A program designed to support a public body manage the personal information it collects, manages, uses, and discloses. A privacy management program must consist of documented policies and procedures that promote the public body's compliance with the Act.<br><br>For example, a public body's privacy management program may include processes to collect and store personal information, information retention schedules, information archival processes, and breach response procedures. |
| Public body | 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, or library). |
| Synthetic data | Synthetic data is artificially created through computer simulation or algorithms to maintain the structure and patterns of real data but is not linked to any individual in the original data set. Synthetic data mirrors real-world data without including individuals' personal information. |