Fact Sheet: Key differences between the POPA and the FOIP Act

The new *Protection of Privacy Act* (POPA) has incorporated new provisions, as well as revised provisions from the *Freedom of Information and Protection of Privacy Act*, aimed at enhancing clarity, strengthening regulatory accountability, and implementing administrative updates. Some of the key differences include:

Definitions

Numerous definitions have been revised or added into the Act. Some notable ones include:

Personal Information

The definition was expanded under subsection (i) to now also include “home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual’s employer or principal in the individual’s capacity as an employee or agent.” Subsection (iii) was expanded to include “gender identity”, as well as “sexual orientation”, and subsection (vi) was reworded to “the individual’s physical or mental health”.

Business day

Under the Act, a “day” is now defined as a “business day”.

Business day means a day other than a Saturday, a holiday, or a day when Government of Alberta offices are closed as part of the Government of Alberta’s Christmas closure.

Common or integrated program or service

These are defined as a program or service planned, administered, delivered, managed, monitored, or evaluated by the public body working collaboratively with one or more other public bodies or another public body working on behalf of the public body, or the public body and one or more other public bodies.

These are formally integrated into multiple sections of the Act including the Collection of Personal Information, and the Disclosure of Personal Information.

See “Common or Integrated Program” Fact Sheet.

Collection of personal information

A public body may indirectly collect personal information if the information is necessary to plan, administer, deliver, manage, monitor, or evaluate a common or integrated program or service.

Public bodies must also notify individuals if they have any intention to input their personal information into an automated system to generate content or make decisions. This keeps Albertans informed and aware of how their personal information is being used to provide services and programs.

Correction of personal information

The timeline for responding to a request to correct personal information can only be extended by the Commissioner, and the timelines involving prescribed days for both correcting and transferring correction of personal information requests have been changed from “days” to “business days”.

See “Correction of Personal Information” Fact Sheet.

Breach notification

Public bodies must give notice when privacy breaches with a real risk of significant harm occur. In those instances, they must give notice, without unreasonable delay, of the incident to the individual to whom there exists a real risk of significant harm, as well as to the Commissioner, and to the Minister.

See “Privacy Incident Notification” and “Privacy Incident Response” Fact Sheets.

The sale of personal information

Section 11 prohibits public bodies from selling the personal information in their custody or under their control.

Disclosure of personal information

Numerous subsections were removed, and subsection (ff) was added under section 13 indicating that a public body may disclose personal information to another public body for the purpose of carrying out data matching to create data derived from personal information under section 17(1).

Data matching

Data matching is defined as linking personal information between two or more databases or other electronic sources of information.

Section 17 of the Act sets out the rules related to data matching by a public body. This section did not previously exist under FOIP.

See “Data Matching and Data Derived from Personal Information” Fact Sheet.

Data derived from personal information

Data derived from personal information means data created by data matching and identifies any individual whose personal information was used in the data matching. Both elements of the definition need to be met in order to be considered data derived from personal information, meaning it must be the merging of two or more sources to create new information about an individual and that the personal information in the data must still be identifiable.

Sections 18 to 20 of the Act did not previously exist under the former FOIP Act and pertain to the retention, use, disclosure, and protection of data derived from personal information.

See “Data Matching and Data Derived from Personal Information” Fact Sheet.

Non-personal data

Non-personal data means data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the regulations.

Section 21 to 24 of the Act did not previously exist under FOIP and pertain to the creation, use, disclosure, and protection of non-personal data.

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.

See “Creation and Use of Non-Personal Data”, and “Disclosure of Non-Personal Data” Fact Sheets.

Privacy management programs

Part of the way that a public body fulfills its obligation to protect personal information, data derived from personal information, and non-personal data in its custody or under its control is to have a privacy management program which is open and transparent.

Section 25 of the Act sets out the requirement for public bodies to implement a privacy management program.

See “Privacy Management Program” Fact Sheet.

Privacy impact assessments

Conducting privacy impact assessments is an exercise to assist public bodies in identifying and addressing privacy risks associated with the implementation of any new administrative practice, program, project or service.

Section 26 of the Act sets out the requirement that public bodies be required to prepare privacy impact assessments under certain circumstances.

See “Privacy Impact Assessments” Fact Sheet.

The Information and Privacy Commissioner

The OIPC was granted powers that correspond with the additions to the Act in order to streamline operations and hold public bodies to account. They may:

- Comment on the implications for protection of privacy related to data matching practices, data derived from personal information and non-personal data
- Order public bodies to stop activities related to data matching, data derived from personal information, or non-personal data if the organization is operating in contravention of the Act
- Choose not to proceed with an investigation unless the applicant wants them to or if the OIPC deems it unnecessary
- Require a public body to provide them with a copy of their privacy impact assessments or privacy management program

Stronger penalties

Where an individual knowingly contravenes the Act there can be consequences that lead to fines. Where a contravention is suspected, the Information and Privacy Commissioner will review and investigate the matter and could make recommendations to prosecute.

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 3 of the Act, which relates to data matching and non-personal data.