Protection of Privacy Act

Guide

Contents

Protection of Privacy Act
Overview

Purpose

The *Protection of Privacy Act* (POPA) is an authority-based legislation that governs the protection of privacy related to personal information in the custody or under the control of Alberta public bodies. The protection of privacy requires accountability, compliance and transparency on how public bodies are protecting personal information, data derived from personal information, and non-personal data.

Under section 2, the purposes of the Act are to:

- Control the collection, use and disclosure of personal information by a public body,
- Allow individuals a right to request corrections to personal information about themselves,
- Control the creation, use and disclosure of data derived from personal information and non-personal data by a public body, and
- Provide for independent reviews of decisions made by public bodies under this Act and the resolution of complaints under this Act.

Scope

POPA applies to all public bodies in Alberta. The *Access to Information Act* (ATIA) section 1(t) and its accompanying Designation of Public Bodies Regulation define and provide a complete listing of public bodies that are subject to POPA. This means all public bodies as defined in the ATIA have statutory duties under POPA, unless a specific exclusion applies.

Public bodies include:

- a department, branch or office of the Government of Alberta;
- an agency, board, commission, corporation, office, or other body designated as a public body in the regulations (Designation of Public Bodies Regulation);
- the Executive Council Office;
- the office of a member of the Executive Council;
- the Legislative Assembly Office;
- the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, Information and Privacy Commissioner, the Child and Youth Advocate or the Public Interest Commissioner;
- or a local public body including educational bodies, health care bodies and local government bodies.

The Act applies to all personal information collected, used or disclosed by a public body and all data derived from personal information and non-personal data created, used or disclosed by a public body. However, some records and information are excluded from POPA altogether, meaning they are not subject to any provisions under the Act such as: personal information contained in, or data derived from personal information or non-personal data contained in or created from: court files, records created by officers of the Legislature in the course of their duties,

information collected, used or disclosed by public registries (e.g. Land Titles Offices, Registrar of Vital Statistics, etc.), etc. For more information on records that are excluded from POPA, please refer to section 3 of the Act.

Paramountcy

The POPA does not include an express paramountcy provision. Instead, it provides the head of a public body with discretion to determine whether to disclose personal information under the Act.

POPA authorizes the collection and disclosure of personal information (specifically sections 4(a), 13(1)(d) and (e) of the Act) when authorized or required by another enactment. As such, there should not be a conflict between POPA and another legislation.

The only exceptions in POPA that provide paramountcy are sections 19(4) and 23(4), which grant paramountcy to POPA's disclosure provisions for data derived from personal information and non-personal data respectively over the ATIA. Meaning data derived from personal information and non-personal data are not accessible through a formal access to information request to ensure the protection of these types of information and data.

Regulations

There are two Protection of Privacy Regulations that establish administrative and procedural requirements of the Act:

- Protection of Privacy Regulation, authorized by the Lieutenant Governor in Council, contains provisions pertaining, but not limited to: defining terms not already defined in POPA and respecting any other matter the Lieutenant Governor in Council considers necessary.
- Protection of Privacy (Ministerial) Regulation, under the authority of the Minister of Technology and Innovation, contains provisions pertaining, but not limited to: requirements for Privacy Incident Reporting, Privacy Impact Assessments and Privacy Management Programs.

POPA and its regulations work together to provide detailed, practical guidance to help public bodies implement the new rules.

Roles and Responsibilities

Overview

All public bodies have responsibilities under POPA, these include ensuring the protection of personal information, data derived from personal information, and non-personal data from risks such as unauthorized access, collection, use, disclosure, or destruction, among other duties.

More specifically, compliance with POPA involves various roles and responsibilities that can be broken down accordingly:

Minister

The Minister of Technology and Innovation is responsible for POPA. As the Minister with responsibility for the Act, Technology and Innovation leads administration, legislative updates and preparation of an annual report on the operation of the Act (see section on Annual Reporting).

Head of a public body

The head of each public body is responsible for decisions made under POPA and the protection of privacy, as they relate to that public body. Section 1(h) of the ATIA defines “head” in relation to a public body. This definition applies to any use of the term under POPA.

Under POPA, the head of a public body may delegate powers and duties to another employee or employee of a public body under section 55. The only power that cannot be delegated is the power itself to delegate.

Delegation by head of public body

The delegation of powers by a head of a public body must be in writing and identify the position, not the individual, to which the powers are delegated. This ensures that the delegation remains valid and effective when a new person assumes the position or when someone is acting in that capacity. The delegation instrument may include any conditions or limitations the head considered appropriate. Additionally, it can provide for the delegation to transfer to another position if the original delegate is absent or incapacitated. A delegation instrument may cover a wide variety of duties, powers and functions under POPA.

It is important to review the instrument periodically for any changes that may be needed, especially if the public body is restructured or part of the public body is transferred to another public body.

For more information see the Fact Sheet: Delegations and template.

Privacy Officer and Privacy Office

The Privacy Officer is the designated employee that handles the day-to-day operations of POPA and is responsible for the public body’s compliance with the Act. The designation of a Privacy Officer is a requirement of the privacy management program for public bodies, as per the Protection of Privacy (Ministerial) Regulation. Refer to the Privacy Management Programs section below for more information.

There are various aspects of the Privacy Officer’s position that may vary depending on the size of the public body, the delegated authorities, and the volume and sensitivity of personal information, data derived from personal information and non-personal data handled by the public body.

For some public bodies, the structure may include a full time Privacy Officer with additional staff in a Privacy Office, while smaller public bodies may have an officer that only works in that capacity on an “as needed” basis.

The Privacy Officer or Office should be the focal point for protection of privacy expertise within the public body.

Employees

Employees, as defined in section 1(h) of POPA, in the context of a public body includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body. This means that contractors and other individuals providing a service to a public body are required to be compliant with the POPA and understand their responsibilities under the Act. Training requirements ensure these individuals understand their responsibilities.

POPA requires the head of the public body to be responsible for protecting certain types of information and making certain decisions under the Act, including responding to requests for the correction of personal information, and privacy incident notifications. However, all employees play an important role in ensuring compliance with POPA through their day-to-day work. Public body heads or delegated decisions makers should be fully informed of POPA matters to make appropriate decisions and the obligation to raise concerns rests with all employees.

Employees are responsible for:

- Understanding their roles and responsibilities under POPA;
- Protecting personal information, data derived from personal information, and non-personal data against such risks as unauthorized access, collection, use, disclosure or destruction;
- Completing any required trainings related to their privacy protection obligations;
- Adhering to their public body’s privacy management program’s policies and procedures;
- Ensuring any collections/uses/disclosures of personal information are authorized under the Act, and done only to the extent necessary to complete their job duties;
- Ensuring any creations/uses/disclosures of data derived from personal information and non-personal data are done in accordance with the Act;
- Following policies and processes for the completion of Privacy Impact Assessments to ensure that any programs, administrative practices, etc., involving personal information or data derived from personal information, comply with the privacy protection provisions of the POPA;
- Notifying and working with their supervisor and other parties as required, to assist with the investigation process in the event of a privacy incident;
- Responding to correction to personal information requests in accordance with their public body’s policies;
- Ensuring the appropriate agreements, safeguards or other compliance mechanisms are in place prior to collecting, using or disclosing personal information, data derived from personal information or non-personal data.

Knowingly contravening POPA is considered an offence under the Act. Employees found knowingly contravening POPA may face further investigation by Alberta’s Information and Privacy Commissioner, and penalties based on the offence. Please see the Offences and Penalties section below for more information.

Contractors

Public bodies must also ensure that contractors, volunteers, students or other individuals providing services on behalf of the public body follow proper protection procedures and adhere to their responsibilities under POPA

based on their particular job responsibilities. When contracting for services involving personal information, data derived from personal information or non-personal data, public bodies should incorporate privacy protection provisions in the agreement or contract between the public body and the contractor. If you are unsure whether your contracts are in-line with POPA compliance, please contact your public body's Privacy Officer or Office, or your legal counsel for assistance.

Personal Information

Overview

Personal information is defined under POPA as “recorded information about an identifiable individual.” Some examples include:

- The individual’s name, home or business address, or other contact information, except where the individual provided the information on behalf of their employer in their capacity as an employee or agent;
- The individual’s race, national or ethnic origin, colour or religious or political beliefs or associations;
- The individual’s age, gender identity, sex, sexual orientation, marital status or family status;
- An identifying number, symbol other particular assigned to an individual,
- The individual’s’ fingerprints, or other biometric information,
- The individual’s personal views or opinions, except if they are about someone else.

See section 1(q) of POPA for the specific definition for personal information which is not an exhaustive list. Any recorded information that identifies an individual is considered personal information.

Personal information must be collected, used, disclosed, secured and retained in accordance with the provisions of POPA unless the information is outside the scope of the Act (see section 3 for a list of excluded records).

As POPA is an authority-based legislation, personal information may only be collected, used and disclosed if a provision or legal authority specifically authorizing such activity exists in the Act. If you are not certain whether you have authority to collect, use or disclose personal information, reach out to your public body’s Privacy Officer/Office.

Collection of personal information

Section 4 of POPA sets out the only circumstances under which public bodies are authorized to collect personal information. A public body can only collect the personal information that is directly related to and necessary for the program or activity, or is authorized by an enactment of Alberta or Canada or the personal information is collected for the purposes of law enforcement.

If no provision authorizing the collection of personal information applies, public bodies cannot collect it.

A public body is bound by the requirements of the Act regardless of whether it conducts the collection itself, or an outside agent (under contract or through an agreement/arrangement) carries out the collection on the public body’s behalf.

Collection occurs when a public body gathers, acquires, receives or obtains personal information which may be done through forms, interviews, questionnaires, surveys, polling, video surveillance, etc. The legislation does not restrict the format by which personal information is collected, so information may be collected in writing, by audio or video, electronic data entry, via an automated system or other means.

Manner of Collection

Subject to limited exceptions, public bodies must collect personal information directly from the individual it is about as per section 5(1). This helps ensure transparency to individuals so they are aware of the type of personal information being collected and the purpose. It also allows the individual to challenge the need for the information or refuse to provide the information or participate in the program or activity.

A public body must not seek or passively receive the personal information from another source even though it may have the capability of doing so, unless collection from that indirect source or for that purpose is authorized in the exceptions listed under section 5(1).

Please refer to section 5(1) for a full list of exceptions. These exceptions authorize a public body to collect information indirectly, be it from another public body, individual or organization under specific circumstances.

Collection Notices

When a public body collects personal information directly from the individual the information is about, section 5(2) requires them to give notice to the individual, at the time of collection of:

a) The purpose for the collection (i.e., the reason for which the information is being collected);
b) The specific legal authority for the collection (i.e., the specific section(s) that authorizes the collection for that identified purpose);
c) Contact information to which the individual may direct any questions they have about the collection;
d) The public body's intention, if any, to input the information into an automated system to generate content or make decisions, recommendations or predictions.

If, at the time of collection, a public body also intends to input personal information into an automated system to generate content or make decisions, recommendations or predictions, this needs to be specified in the collection notice. An Automated System is any system, software, or process that uses computation as a whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities. For more information on automated systems refer the Fact Sheet: AI and Automated Systems.

A collection notice allows the individual to understand the purpose of the collection, and how the information will be used, and make an informed decision about whether they wish to proceed in providing the information. For more information see the Fact Sheet: Collection Notices.

Additional Exceptions

There may be certain limited circumstances under which collecting information directly or notifying individuals of the purpose of collection may lead to the collection of inaccurate information. In those cases, section 5(3) permits public bodies to set the requirements under section 5(1) and 5(2) aside. This exception should only be used in limited circumstances and public bodies should document when the provision is used, and for what reason.

Lastly, if a public body has already provided a collection notice to an individual, and they continue to collect personal information from that individual, they are not required to give notice to the individual every time, provided the purpose and specific legal authority have not changed from the original notice (section 5(4)).

Use of personal information

Section 12 of the Act lists the only circumstances under which a public body may use personal information. If no provision authorizing the use of personal information applies, public bodies cannot use it.

Use of personal information means employing it to accomplish the public body's purposes, for example, to administer a program or activity, to provide a service or to determine eligibility for a benefit. See section 12 of POPA for a full list of circumstances under which personal information may be used.

When using personal information, public bodies must ensure they use only what is necessary to carry out its purpose in a reasonable manner (section 12(4)). This provision applies to both the amount and type of personal information being used and is intended to ensure that public bodies use the minimum amount of information necessary to achieve their purposes.

Disclosure of personal information

Section 13 of the Act sets out the circumstances under which a public body is authorized to disclose personal information. Some examples include:

a) if the disclosure would not be an unreasonable invasion of personal privacy under section 20 of the Access to Information Act,
b) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
c) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure.

Refer to section 13 of POPA for a full list of circumstances under which personal information may be disclosed. If no provision authorizing the disclosure of personal information applies, public bodies cannot disclose it.

Disclose means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information by any means to someone. In this context it includes: oral transmission by telephone or in person; provision of personal information on paper, by fax or mail; and electronic transmission through email, data transfer or the internet.

POPA does not specify the manner in which disclosure must occur. Disclosure can occur both orally or in writing and should be made in a way that helps the requester and is cost-effective for the public body. To help determine the best method of disclosure, consider the sensitivity of the information, the relationship with who it will be disclosed to, and the type of disclosure.

Lastly, section 13 enables disclosure; it does not require disclosure. Just as when collecting or using personal information, public bodies must ensure they disclose only what is necessary to carry out its purpose in a reasonable manner (section 13(4)).

Consistent Purpose

A public body is authorized under section 12(1)(a) and 13(1)(b) to use or disclose personal information, respectively, for the purpose for which the information was [originally] collected or compiled or **for a use *consistent* with that purpose**.

Section 14 of POPA states that a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure:

- Has a reasonable and direct connection to that purpose, and
- Is necessary for performing the statutory duties of, or for operating a legally authorized program or common or integrated program or service of, the public body that uses or discloses the information.

A use or disclosure has a ***reasonable and direct connection*** to the original purpose if there is a logical and plausible link to the original purpose. A consistent use should grow out of or be derived from the original use; it should not be an unrelated or secondary use of the information.

A use or disclosure is ***necessary for performing the statutory duties of, or for operating a legally authorized program or common or integrated program or service*** if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed.

For a use or disclosure to be considered consistent, both of the above conditions must be met.

An example of a consistent purpose includes:

- *Evaluation of a program* - public bodies will have a regular need to evaluate the operation and success of their programs. This is particularly true of new programs or those that have changed in some way. Section 14 allows a public body to select clients or participants who can participate in that evaluation through questionnaires or interviews.

Consent

As POPA is authority-based, a public body does not require consent to use or disclose personal information except when it relies on sections 12(1)(b) or 13(1)(c), as its authority to do so.

- Section 12(1)(b) permits public bodies to use personal information if the individual to whom the information pertains has both identified the specific information and provided consent, in the prescribed manner, for its use for a particular purpose.
- Section 13(1)(c) authorizes public bodies to disclose personal information under the same conditions as section 12(1)(b), with the key difference being the substitution of the term “use” with “disclosure.”

Both sections specify that consent must be obtained “in the prescribed manner.” This means that the consent is only valid if the public body has met all the applicable requirements for obtaining consent as set out in section 2 of the Protection of Privacy Regulation.

Common or Integrated Programs or Services

Public bodies may implement programs or services that require collaboration and/or are in partnership with other public bodies. A ***common or integrated program or service*** is collaboratively planned, administered, delivered, managed, monitored or evaluated by two or more public bodies, or by one public body working on behalf of one or more other public bodies (section 1(d)). Such programs or services may consist of several distinct components, each provided or delivered by a different public body. Together, these components comprise the common or integrated program or service.

When a common or integrated program or service is established, there are requirements that other collection and/or disclosure authorities in POPA do not have, therefore this purpose should be reserved for situations where other POPA authorities for the collection, use and disclosure of personal information are not available or practical.

Under the Protection of Privacy (Ministerial) Regulation, if a practice, program or project or service is part of a common or integrated program or service, the public body is required to complete and submit a Privacy Impact Assessment (PIA) to the Information and Privacy Commissioner as per section 7.

Furthermore, to ensure effective governance and accountability in a common or integrated program or service, this PIA must establish a clear governance structure, outlining each public body’s responsibilities as they relate to

the personal information involved in the program or service, and their compliance with the Act. This ensures each collaborating public body is essential to the program's operation; the program would not function without their contributions.

As a best practice, public bodies implementing common or integrated programs should establish an agreement between public bodies to ensure clarity on roles and responsibilities. These agreements can be attached to PIAs.

For more information on PIA requirements, see the PIA section below. For more information on these programs or services, refer to the Fact Sheet: Common or Integrated Programs or Services.

Accuracy and Retention

Overview

POPA requires that if a public body uses an individual's personal information to make a decision that directly affects the individual, including a decision made using an automated system, the public body must:

- make every reasonable effort to ensure the information is accurate and complete.
- Retain the personal information for at least one year after using it so that the individual has an opportunity to obtain access to it.

Retention may be for a shorter time period under certain conditions stated in section 6(b) of the Act, this allows an individual to review, and if necessary, to request a correction of the information used to make a decision on them, before disposition of that information takes place.

Section 6 does not apply if no decision, adverse or otherwise, will be or has been made about an individual. Examples include raw survey data where personal information is collected but the results are rendered anonymous, telephone messages, and unsolicited résumés that are never considered in relation to a position.

Correction of personal information

Overview

If an individual believes that their personal information, in the custody or under the control of a public body, contains an error or omission, they may request the public body to correct the personal information under section 7 of POPA.

In many cases, an individual will ask for personal information to be corrected and supply proof of correction without doing this in a formal way. Public bodies can, and most often will, make corrections without a request under the Act if this is practical and expedites public business. Otherwise, individuals may submit a formal request for correction of personal information instead.

Regardless of how it is made, the public body has 30 business days to process a request for correction after receiving it, unless otherwise allowed by the Information and Privacy Commissioner.

Processing a request for correction

POPA gives individuals the right to *request* a correction of personal information. However, public bodies may either correct the information, or may refuse, subject to other provisions.

- When a public body decides to ***correct*** an error, either by changing or adding new information, all records containing the personal information must be corrected, and annotated with the date of the correction. The public body may also need to notify other public bodies or third parties unless an exception under section 7(5) of POPA applies.
- If a public body ***refuses or is unable*** to make a correction that an individual requests, it must annotate or link the personal information in question with the relevant part of the requested correction.

The public body may refuse or be unable to make a correction because the information is not personal information, the applicant has not submitted adequate proof in support of the requested correction, or the information consists of an opinion rather than fact.

For more information, refer to the Fact Sheet: Correction of Personal Information.

Transferring a request for correction

When a request for correction is received where another public body originally collected or compiled the personal information, the request should be transferred to that public body for response as per section 8. It must also ensure that all public bodies to which the information was disclosed are properly notified of the correction.

If a request is transferred under this section, the public body transferring the request must notify the individual of the transfer as soon as possible. The public body receiving the transferred request must follow the requirements outlined in Section 7 of POPA. A public body has 30 business days, or longer if approved by the Commissioner, from the date of the transfer to respond to the request for correction.

Privacy Management Requirements

Privacy Management Programs

Under section 25 of POPA, public bodies are required to establish and implement a privacy management program (PMP) consisting of documented policies and procedures that promote the public body's compliance with their duties under the Act.

All public bodies have a responsibility to handle and safeguard personal information, data derived from personal information, and non-personal data in accordance with POPA. Having policies and procedures in place, as part of their PMP, helps ensure public bodies are well equipped to meet this mandate. This, in turn, promotes accountability and transparency, giving individuals the opportunity to understand how their personal information is managed by public bodies.

For more information, refer to the Fact Sheet: Privacy Management Programs.

PMP Requirements

To assist in the establishment and implementation, the Protection of Privacy (Ministerial) Regulation specifies the information public bodies must include in their PMP in section 6 to be compliant with POPA.

However, whether it be due to size, the services they offer, or other factors, public bodies vary in the volume and sensitivity of personal information in their custody or control. Therefore, to enable scalability, section 25(2) of POPA mandates that a PMP must be proportional to the volume and sensitivity of the personal information that a public body manages, provided the prescribed requirements in the regulation are met.

To further enable scalability, section 6(1) of the regulation outlines PMP requirements that apply to all public bodies, while section 6(2) specifies additional requirements applicable only to those that have custody or control of a high volume of personal information, or highly sensitive personal information.

For the purposes of the regulation, section 1 defines the type of information deemed to be of high sensitivity. If a public body has personal information in their custody and control that they consider highly sensitive, they are encouraged to follow the requirements set out in section 6(2). Refer to the Protection of Privacy (Ministerial) Regulation for the full list of requirements.

If you are unsure whether your public body is subject to section 6(2), please contact your public body's Privacy Officer or Office, or your legal counsel for assistance.

Additional PMP Requirements

Other notable requirements listed in the regulation include, but are not limited to:

- Public bodies must establish a process for making their PMP available to the public on request or may instead opt to make them publicly available on their website (section 6(3)).
- If, some of the information contained in a PMP may compromise the security of the personal information in the custody or control of the public body if released, it may be withheld. Section 6(4) authorizes public bodies to withhold such information in accordance with sections 10(1), 20 and 24 under POPA.
- PMPs must be regularly reviewed, assessed and updated by the public body to ensure continued compliance.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a process that assists public bodies in reviewing the impact that a new, or significant change to an existing practice, program, project or service may have on individual privacy if it involves the collection, use or disclosure of personal information. The process is intended to ensure that the public body evaluates the project for compliance with POPA, identifies any possible privacy implications for individuals, and considers possible mitigation strategies and safeguards to reduce or eliminate any negative impact. The PIA provides documented assurance that all privacy issues related to the initiative have been appropriately identified and addressed.

Under certain prescribed circumstances - listed under section 7 of the Protection of Privacy (Ministerial) Regulation - POPA requires public bodies to complete a PIA, and if required by the regulations, submit it to Alberta's Information and Privacy Commissioner (the Commissioner).

For more information see the Fact Sheet: Privacy Impact Assessments.

Internal Completion Process

To assist in their completion, the Protection of Privacy (Ministerial) Regulation specifies the information public bodies must include in a PIA in section 7(2) to 7(4) to be compliant with POPA. This includes identifying the types of personal information involved, the purpose of these activities, the corresponding legal authorities, information flows, etc.

Section 7(3) mandates that the PIA must provide sufficient detail to reflect the complexity of the practice, program, project or service it pertains to. This section aims to ensure scalability, enabling public bodies to adjust the level of detail based on the project's complexity and size. Note: certain PIA provisions are specific to certain types of practices, programs, etc. such as those involving data matching, or that are part of a common or integrated program or service. Refer to the regulation for the full list of requirements.

Not all practices, programs, etc. meet the threshold for requiring a PIA under POPA. Nevertheless, public bodies are recommended to still complete a PIA in alignment with sections 7(1) to 7(4), if a practice, program, etc. involves the collection, use or disclosure of personal information. Adopting this approach as a best practice measure ensures compliance with the Act and the protection of privacy.

As part of the PMP requirements under the Protection of Privacy (Ministerial) Regulation, public bodies that handle a high volume of personal information or highly sensitive information are required to establish their own internal process for completing and submitting PIAs (section 6(2)(a)(ii)). If you are unsure whether your public body falls under this category, please contact your public body's Privacy Officer or Office for assistance. Otherwise, please refer to your public body's PMP, if applicable, and the Fact Sheet: Privacy Impact Assessments for more information.

Submissions to the Commissioner

Apart from the completion criteria, section 7(5) of the Protection of Privacy (Ministerial) Regulation sets out the circumstances under which public bodies are required to submit a PIA to the Commissioner.

Even if submission to the Commissioner is not required, public bodies may choose to submit any PIAs voluntarily, if they wish.

On the submission process, please refer to the OIPC's website for more information on their submission process and any other guidance they provide related to PIAs.

Privacy Incidents

A privacy incident, as described in section 10(2) of POPA, occurs when there is a loss of, unauthorized access to, or unauthorized disclosure of personal information in the custody or control of a public body where there exists a real risk of significant harm (RROSH) to an individual as a result of the incident.

When these incidents occur, POPA requires a public body to give notice of the incident to:

- The impacted individual(s);
- The Information and Privacy Commissioner; and
- The Minister responsible for POPA (the Minister of Technology and Innovation).

Incidents involving data derived from personal information created under section 17 of the Act are subject to the requirements under section 10(2) and 10(3) if it meets the threshold for RROSH. See the data derived from personal information section below for more information.

For a public body, taking appropriate steps to contain an incident, evaluating the level of risk and completing notification in a timely, efficient and coordinated manner minimizes the harm that an incident may cause for the impacted individual, and also for organizations, and public bodies themselves. For guidance on how to manage a privacy incident, refer to the Fact Sheet: Privacy Incident Response.

As part of the PMP requirements under the Protection of Privacy (Ministerial) Regulation, all public bodies are required to establish their own internal policies and procedures for responding to incidents, as described in section 10(2) of POPA. Refer to your public body's policies and procedures or your Privacy Officer/Office for more information.

If there is an incident that does not meet the threshold for RROSH, it is still important that public bodies are keeping track of, responding appropriately to privacy breaches, and taking steps to prevent reoccurrence. This helps public bodies ensure they are meeting their obligations to protect personal information in their custody and control, regardless of whether they are obligated to report or not.

To determine whether notification is mandatory, public bodies must first evaluate the level of risk associated with an incident:

Real Risk of Significant Harm

To determine whether an incident meets the threshold for RROSH, the Protection of Privacy (Ministerial) Regulation identifies the factors constituting "real risk of significant harm" in section 4(1), and what would be considered "significant harm" in section 4(2). As all incidents are unique, public bodies should exercise their judgment on each incident and consider any other relevant factors not listed in the regulation.

For more information on how to determine RROSH, refer to the Fact Sheet: Privacy Incident Notifications. See the OIPC's assessment tool for RROSH for more guidance on the OIPC's website.

Notifications

Any notice given under section 10(2) of POPA must comply with prescribed requirements set out in the Protection of Privacy (Ministerial) Regulation, as per section 10(3), and must be completed through one of the authorized methods listed in section 53 of the Act.

Notification requirements vary between the impacted individual(s), the Commissioner and the Minister, and therefore have been tailored based on each recipient's specific needs. These are outlined in sections 7(3) to 7(5) of the regulation.

For more information, refer to the Fact Sheet: Privacy Incident Notifications for an in-depth discussion on notification requirements and more information on the manner of notification for each recipient.

Data Matching

Overview

Data matching refers to the practice of linking personal information between two or more databases or other electronic sources (section 1(f)). Data matching may be carried out by a single public body, using personal information already in their custody and control, or it could involve more than one public body, for example, if two government ministries align data sets to assess program eligibility. Regardless, the resulting information is referred to as ***data derived from personal information*** (section 1(e)).

To enable data matching, POPA authorizes the collection, use and disclosure of personal information, with restrictions, for the purposes of data matching. Additionally, public bodies are responsible for protecting data derived from personal information created under section 17(1) by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. Therefore, these restrictions help ensure that public bodies balance using data appropriately and ethically to improve their services and programs, with the protection of privacy.

As part of the PMP requirements under the Protection of Privacy (Ministerial) Regulation, public bodies that handle a high volume of personal information or highly sensitive information are required to establish their own internal policies and procedures related to their use of artificial intelligence in creating data derived from personal information (section 6(2)(a)(v)), and for monitoring their systems that hold this data (section 6(2)(a)(iii)).

For more information on data matching and data derived from personal information, refer to the Fact Sheet: Data Matching and Data Derived from Personal Information.

Data derived from personal information

Data derived from personal information identifies any individual whose personal information was used in the data matching (section 1(e)(ii)). Combining this with the information for data matching above, data derived from personal information ultimately consists of personal information about an identifiable individual as defined under section 1(q) of POPA.

As such, the loss of, or unauthorized access to or disclosure of this type of data may also result in significant harm to individuals, etc., falling under the definition of a privacy incident as per section 10(2). Therefore, if an incident involving data derived from personal information meets the threshold for RROSH, public bodies are required to provide notice in accordance with sections 10(2) and 10(3). Please see the Privacy Incidents section above for more information.

In contrast however, although data derived from personal information is made up of personal information, POPA sets out separate authorities for, and limitations on the retention and use of data derived from personal information by a public body in section 18, and on its disclosure under section 19. This means that data derived from personal information is not subject to the retention, use, and disclosure of personal information provisions under sections 6, 12, and 13. Public bodies should take note of this important distinction to ensure compliance with the Act.

Creation of data derived from personal information

Public bodies are only authorized to carry out data matching to create data derived from personal information for one or more of the purposes listed under section 17(1) of POPA including research and analysis, planning, administering, delivering, managing, monitoring or evaluating a program or service or any prescribed purposes listed in the Protection of Privacy (Ministerial) Regulation.

Collection of personal information directly from an individual for the purpose of data matching is expressly prohibited under section 17(3) of POPA. Instead, public bodies must either collect personal information from another public body or use that which they already have in their custody or under their control.

This section does not apply to the Office of Statistics and Information (section 17(4)).

Security Arrangements

When creating data derived from personal information, to help meet their protection of privacy requirements under section 20, public bodies must ensure they meet the applicable security requirements outlined in sections 2 and 3 of the Protection of Privacy (Ministerial) Regulation. These include:

- Assigning a security classification level to the data based on the public body's internal classification system (section 2(1)),
- Applying reasonable security arrangements proportional to the classification level (section 3(1)), and
- Implementing human oversight, auditing and validation measures for any systems used for creating data derived from personal information to ensure the accuracy and reliability of the data (section 3(2)).

For more information on these security arrangements, refer to the Fact Sheet: Data Matching and Data Derived from Personal Information and section 1(1)(c)(i) of the Protection of Privacy Regulation.

PIA Requirements

Under the Protection of Privacy (Ministerial) Regulation, if a practice, program or project or service will involve data matching between two or more public bodies, the public bodies are required to complete and submit a Privacy Impact Assessment (PIA) to Alberta's Information and Privacy Commissioner as per section 7(5)(c).

Furthermore, to ensure effective governance and accountability when data matching involves two or more public bodies, this PIA must establish a clear governance structure, outlining each public body's responsibilities as they relate to the personal information involved in the program or service, and their compliance with the Act (section 7(2)(g)).

To further protect privacy, how this personal information will be securely transmitted, matched, or linked by the public body to generate the data derived from personal information must also be identified in the PIA, alongside any administrative, physical or technical safeguards in place (section 7(2)(e)). For more information on PIA requirements, see the PIA section above.

Retention and Use of data derived from personal information

Data derived from personal information can only be used for the purpose it was originally created and can only be retained for as long as it is needed to fulfill that purpose. Once its purpose is fulfilled, the public body must either destroy the data or convert it into non-personal data (sections 18(1) and (2)). Please refer to the non-personal data section below for more information.

This section does not apply to the Office of Statistics and Information as per section 18(3) of POPA.

Disclosure of data derived from personal information

Public bodies are prohibited from disclosing data derived from personal information except when disclosing the data to the public body that provided the personal information used to create it, if that public body requires it for the same purpose for which it was created (sections 19(1) and (2)).

However, this restriction does not apply when a public body discloses the data to the Office of Statistics and Information, as long as it is for the purposes of the *Office of Statistics and Information Act* (section 19(3)).

This section is paramount over the access provisions of the ATIA as per section 19(4) of POPA.

Non-Personal Data

Overview

Non-personal data refers to 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 (section 1(n)). The creation of non-personal data is authorized under section 21 of POPA.

POPA authorizes the creation, use and disclosure of non-personal data with restrictions. Additionally, public bodies are responsible for protecting non-personal data created under section 21(1) by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. Therefore, these restrictions help ensure that public bodies balance using data appropriately and ethically to improve their services and programs, with the protection of privacy.

As part of the PMP requirements under the Protection of Privacy (Ministerial) Regulation, all public bodies are required to establish their own internal policies and procedures for creating non-personal data (section 6(1)(b)(ii)). Public bodies that handle a high volume of personal information or highly sensitive information must also establish such policies and procedures related to their use of artificial intelligence in creating non-personal data under section 6(2)(a)(v), and for monitoring their systems that hold non-personal data (section 6(2)(a)(iii)).

For more information, refer to the Fact Sheet: Creation and Use of Non-personal Data and the Fact Sheet: Disclosure of Non-personal Data.

Creation of non-personal data

The creation of non-personal data is authorized under section 21 only for one or more of the following purposes: for research and analysis, planning, administering, delivering, managing, monitoring or evaluating a program or service, or any prescribed purposes listed in the Protection of Privacy (Ministerial) Regulation.

When creating non-personal data, a public body may only use personal information or data derived from personal information that is already in their custody or under their control (section 21(3)), and this creation must be done in accordance with generally accepted best practices and any prescribed requirements under the accompanying regulations (section 21(2)). Refer to section 5(1) of the Protection of Privacy (Ministerial) Regulation for a full list of requirements.

Each time a public body creates non-personal data, it must maintain a record that includes:

- a description of the personal information or data derived from personal information used to create the non-personal data,
- the purpose for creating the non-personal data,
- the method used for creating the non-personal data, and
- the assessment done to ensure that the identity of the individual who is the subject of the non-personal data cannot be identified or re-identified from the data.

The assessment must contain all the information described in section 5(2) of the regulation, as per section 5(3).

These records should be retained by the public body to ensure questions on the creation of non-personal data can be reviewed where there are concerns related to re-identification or other possible contraventions of POPA. Appropriate record-keeping is essential for transparency in the creation, use and disclosure of non-personal data.

Section 21(3) does not apply to the Office of Statistics and Information as per section 21(3.1) of POPA.

Security Arrangements and Data Quality Assurance

When creating non-personal data, to help meet their protection of privacy requirements under section 24, public bodies must ensure they meet the applicable security requirements outlined in sections 2 and 3 of the Protection of Privacy (Ministerial) Regulation. These include:

- Assigning a security classification level to the data based on the public body's internal classification system (section 2(1)),
- Applying reasonable security arrangements proportional to the classification level (section 3(1)), and
- Implementing human oversight, auditing and validation measures for any systems used for creating non-personal data to ensure the accuracy and reliability of the data (section 3(2)).

As per section 5(1), when creating non-personal data, public bodies must also establish a data quality assurance process in order to:

- Verify and review the effectiveness of any methods used to create the non-personal data, and ensure they can be replicated for auditing purposes,
- Identify and account for potential bias in the data, and
- Ensure the accuracy and completeness of the data if it will be used to inform decisions about programs or services.

For more information on these security arrangements and the data quality assurance process, refer to the Fact Sheet: Creation and Use of Non-personal Data and section 1(1)(c) of the Protection of Privacy Regulation.

Use of non-personal data

There are no restrictions on how a public body can use non-personal data it has created. However, before it uses this data, it must conduct an assessment to determine the level of risk of reidentification in accordance with section 5(2) of the regulation.

Disclosure of non-personal data

Section 23(1) of POPA authorizes the disclosure of non-personal data created under the Act to another public body for any purpose.

It also authorizes a public body to disclose non-personal data to a person other than a public body (i.e. third party) under certain circumstances. Where a public body is considering disclosing non-personal data to a third party, disclosure is only authorized for one or more of the following purposes: research and analysis, planning, administering, delivering, managing, monitoring or evaluating a program or service, or when prescribed by the regulations.

If this non-personal data is being disclosed to a third party, the head of the public body and the third party must sign an agreement under section 23(1)(b)(ii) detailing:

- the security and confidentiality requirements for the non-personal data,
- the prohibition of any actual or attempted re-identification of the non-personal data,
- the prohibition of any subsequent use or disclosure of the non-personal data without the express authorization of the public body, and

- the destruction of the non-personal data at the earliest reasonable time after it has served its purpose.

Any agreement needs to comply with POPA, its accompanying regulations and any of the public body's policies and procedures relating to non-personal data.

Additionally, before disclosing non-personal data, a public body must first conduct an assessment in accordance with section 5(2) of the regulation.

Finally, section 23 of POPA does not restrict the disclosure of any reports, summaries, or other publications containing non-personal data that is in aggregate or statistical form. Refer to the Fact Sheet: Disclosure of Non-personal Data for additional information.

This section is paramount over the access provisions of the ATIA as per section 23(4) of POPA.

Complaints on collection, use and disclosure

Overview

An individual who believes their personal information has been collected, used or disclosed by a public body in contravention of this Act can request the Information and Privacy Commissioner to review their complaint under section 37(1), if the public body concerned does not respond under subsection (3) to the complaint made under subsection (2) by the person asking for the review, within 60 business days after the end of the period set out in subsection (3).

The following is a general overview of the request for review/complaint process. For more information on this process, refer to sections 37 to 44, or the OIPC's website.

Contacting the Public Body

In accordance with section 38(2), individuals must first direct their complaint to the public body that is the subject of their complaint. To support this process, public bodies should ensure their websites provide clear guidance on how to submit their complaint to the public body. This includes prominently displaying contact information for their Privacy Officer or Privacy Office.

Public Body Response

Public bodies are not required under POPA to respond to complaints made by the individual requesting the review. However, if a public body decides to do so, it has 30 business days after it receives the complaint to respond to the individual.

When a complaint is received, a public body should complete an internal review to see if the complaint is founded or whether the collection, use or disclosure was authorized under the Act. Complaints can be useful in helping public bodies ensure their practices comply with the authorities under POPA and could lead to further investigations related to privacy incidents.

Request for Review

Where a public body does an internal review and responds to a complainant, if the individual is not satisfied with the response from the public body, or does not receive a response, they can request a review of the matter by the Information and Privacy Commissioner. For more information on this please see the Role of the Information and Privacy Commissioner section below or refer to the review process on the OIPC's website.

Role of the Information and Privacy Commissioner

Overview

The Information and Privacy Commissioner is an Officer of the Legislature and is independent of government. The Commissioner is appointed by the Lieutenant Governor in Council on the recommendation of the Legislative Assembly under the *Access to Information Act* for a term not exceeding 5 years and is eligible for reappointment.

The Information and Privacy Commissioner is responsible for the oversight and enforcement of POPA. Their role is to provide for independent reviews of decisions made by public bodies, and the resolution of complaints, both under the Act.

General Powers

Under section 27 of POPA, the Information and Privacy Commissioner may:

- Conduct investigations to ensure compliance with any provision of the Act or compliance with rules relating to the destruction of records.
- Make an order regarding duties imposed by the Act, time extensions, or fees, regardless of whether a request for review is requested,
- Inform the public about this Act,
- Receive comments from the public concerning the administration of the Act,
- Engage in, or commission research into anything affecting the achievement of the purposes of the Act,
- Comment on the implications for protection of personal privacy of proposed legislative schemes or programs,
- Comment on implications for protection of personal privacy from data matching and creating, using and disclosing non-personal data,
- Authorize the collection of personal information from sources other that the individual the information is about,
- Give advice and recommendations on the general application to the head of a public body on matters respecting the rights or obligations of a head under the Act,
- Request a copy of a privacy impact assessment of a public body, and
- Investigate and attempt to resolve complaints made under the Act.

For more information refer to the OIPC's website.

Reviews and Complaints

Individuals can request that the Information and Privacy Commissioner review a complaint if they believe a public body is not compliant with POPA (section 37). Where a request for review or inquiry is received, the Information and Privacy Commissioner is responsible for reviewing the complaint. For more information refer to the OIPC's website.

Information and Privacy Commissioner's Orders

If, following a request for review by an individual under section 37, the matter is not settled, the Commissioner must conduct an inquiry, unless, in the opinion of the Commissioner, the circumstances warrant refusing to conduct an inquiry for one or more reasons under section 41(2).

Upon completion of an inquiry however, section 42 requires the Commissioner to make an Order.

The Information and Privacy Commissioner, by order, may:

- Require that a duty imposed by the Act or regulations be performed,
- Require a public body to stop collecting, using or disclosing personal information in contravention of Part 1,
- Require the head of a public body to destroy personal information collected in contravention of the Act,
- Confirm a decision not to correct personal information or specify how it is to be corrected,
- Require a public body to stop collecting personal information for the purposes of carrying out data matching,
- Require a public body to stop carrying out data matching,
- Require a public body to stop using or disclosing data derived from personal information,
- Require a public body to stop creating or disclosing non-personal data, and
- Require the head of a public body to destroy data derived from personal information or non-personal data created in contravention of the Act.

Duty to comply with orders

Upon receipt of an Order made under the Act, the head of a public body must comply with the order or request a judicial review of the decision by the Court of King's Bench within 45 business days from the date of the original order. An individual may request a judicial review of the decision during this period as well.

Where a public body or an individual does not request judicial review, the public body has 50 business days to comply with the order of the Information and Privacy Commissioner.

Offences and Penalties

Overview

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.

An offence occurs where anyone knowingly:

- Collects, uses or discloses personal information in contravention of Part 1,
- Gains or attempts to gain access to personal information in contravention of the Act,
- Collects personal information for the purpose of carrying out data matching in contravention of Part 3,
- Carries out data matching, uses or discloses data derived from personal information in contravention of Part 3,
- Creates or discloses non-personal data in a manner that contravenes section 21(3),
- Gains or attempts to gain access to data derived from personal information or non-personal data in contravention of this Act,
- Re-identifies or attempts to re-identify non-personal data created under section 21(1),
- Makes false statements to mislead or attempt to mislead the Commissioner or someone working on their behalf,
- Obstructs the Commissioner or someone working on their behalf from performing their powers, duties or functions
- Fails to comply with an order,
- Discloses personal information, data derived from personal information or non-personal data to which this Act applies in accordance with a subpoena, warrant or order issued by a court, person or body that has no jurisdiction in Alberta, or in accordance with a rule of court not binding in Alberta.

Fines for an offence can reach up to $125,000 in the case of an individual or up to $750,000 in the case of any other individual where the contravention is in relation to Part 1 of the Act. Where an offence relates to the data provisions under Part 3, fines can reach up to $200,000 for an individual or up to $1,000,000 in the case of any other person.

Under section 59(1), POPA protects an employee of a public body from adverse employment action as a result of properly disclosing personal information, data derived from personal information or non-personal data in accordance with this Act. Anyone who contravenes section 59(1) is guilty of an offence and liable to a fine not more that $10,000.

Annual Report

Purpose

The Minister of Technology and Innovation is responsible for preparing and submitting an annual report on the operation of POPA to the Legislative assembly under section 56 of POPA.

Each annual report covers the fiscal year for the period of April 1 through March 31, and outlines some of the year's highlights and accomplishments. The annual report provides an overview and breakdown of the administration of the Act and the regulations by Alberta public bodies.

Collection of Statistics

On an annual basis, public bodies will be requested to submit their statistics on POPA compliance for the fiscal year. This collection process commences with an initial email sent to all public bodies that requests stats.

More information on what information the annual report will include, and what public bodies will be requested to provide will be shared once it is available.

Development of Annual Report

The statistics collected from Alberta public bodies will be compiled and used to develop the annual report. Once the report is complete, the Minister of Technology and Innovation tables the report in the Legislative Assembly in accordance with the POPA.