Fact Sheet: Consent for Use or Disclosure

The *Protection of Privacy Act* (POPA) requires a public body to obtain consent "in the prescribed manner" for the use or disclosure of personal information under specific and limited circumstances.

Authority-Based Legislation

POPA is authority-based, meaning a public body may only collect, use or disclose personal information if a particular section of the Act authorizes it. A public body may not collect personal information solely based on consent. Consent is also not necessarily required for a public body to use or disclose personal information.

Consent is only required under POPA in limited circumstances when a public body relies on:

- **Section 12(1)(b)** – for the use of personal information.
- **Section 13(1)(c)** – for the disclosure of personal information.

There are many legal authorities for use and disclosure of personal information under the Act. Consent should be used only as a last resort when no other legal authority applies.

Consent for Use or Disclose

Section 12(1)(b) authorizes a public body to use personal information if the individual whom the information is about has identified the specific information, and provided consent, in the prescribed manner, for its use for a particular purpose.

Section 13(1)(c) authorizes a public body to disclose personal information if the individual whom the information is about has identified the specific information, and provided consent, in the prescribed manner, for its disclosure for a particular purpose.

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.

Consent Standards

Consent can be obtained in writing, electronically, or orally. The Protection of Privacy Regulation prescribes specific requirements for each method under subsections 2(3), (4) and (5) respectively. Public bodies may choose the form of consent that best suits their needs, provided all relevant requirements are met.

Public bodies must allow written consent, even if they choose to accept electronic or oral consent. Similarly, they are not obligated to accept consent in electronic or oral form.

Regardless of the method used, there are certain requirements common to all three forms of consent. As per section 2(2), the consent must:

- Meet the requirements of subsection (3), (4) or (5),
- Specify the personal information to which the consent relates,
- Specify to whom the personal information may be disclosed and how the personal information may be used, and
- Specify the date on which the consent is effective, and if applicable, the date on which the consent expires.

As a best practice, public bodies should use plain and simple language to promote accessibility and transparency.

Written Consent

Written consent refers to consent given on paper. For it to be valid, it must be signed by the individual who is giving the consent, as per section 2(3), i.e., it requires a physical (wet) signature.

Electronic Consent

Electronic consent, as per section 2(1)(b), refers to consent provided by electronic means, i.e., where the format is digital or in some other intangible form. Refer to section 2(1)(a) for the full definition of "electronic."

To be valid, electronic consent must comply with all requirements under section 2(4).

Policy Requirements for Electronic Consent

Public bodies are in the best position to determine when it is appropriate to accept electronic consent, based on their specific business needs, and that of the public they serve.

In accordance with section 2(4)(a), each public body must establish a formal policy or "rules" – approved by its head – outlining the specific purposes for which electronic consent will be accepted. Employees of the public body may only seek electronic consent for those approved purposes (section 2(4)(b)).

When developing this policy, public bodies should examine their programs and services, and consider factors such as:

- How is personal information used or disclosed?
- Would the personal information be considered of high-sensitivity (i.e. biometric information, financial information or be respecting a minor, senior or vulnerable individual)?
- Who will the information be disclosed to?
- What risks are associated with accepting electronic consent in those circumstances?
- How feasible is it to obtain electronic consent and ensure it meets the requirements in those circumstances?

Public bodies must also explicitly communicate to the public the specific purposes for which electronic consent will be accepted (section 2(4)(c)).

Technical Requirements for Electronic Consent

As per section 2(4)(d), electronic consent must:

- Be accessible to the public body for future reference/use,
- Be capable of being retained by the public body,
- Be able to be authenticated so the individual giving consent can be identified, and
- Meet the information technology standards, if any, set by the public body.

The methods by which public bodies must fulfill these requirements – such as retention, authentication, or the duration for which electronic consent must remain accessible – are not prescribed in the regulation. These methods may vary depending on the electronic format used, and the business needs of the public body.

Electronic Signature

Electronic consent must include the electronic signature of the individual giving consent (section 2(4)(e)).

Section 2(1)(c) defines electronic signature as:

…electronic information that an individual creates or adopts in order to sign a record and that is in, attached to or associated with the record.

To be valid, the electronic signature must meet the reliability requirements set out in section 16(2) of the *Electronic Transactions Act*. In essence,

- It must reliably identify the individual providing consent, and
- Its association with the relevant record is reliable for the purpose for which the record was created.

The latter overlaps with section 2(4)(g) its association with the consent must be appropriate for the intended purpose.

Subsection (g) acknowledges that the level of sophistication required from the electronic signature may vary depending on the situation. For example, a signature in an internal email may be reliable enough for routine purposes, however, uses or disclosures personal information considered to be high-sensitivity may require more advanced signatures, such as in a public key signature system - a more reliable method.

Oral Consent

Oral consent refers to consent obtained verbally from the individual giving the consent in person, over the phone, video call or recording, etc.

To be valid, consent that is given orally must comply with all requirements under section 2(5), many of which are identical to those for electronic consent.

Policy Requirements for Oral Consent

Sections 2(5)(a) to (c) establish the same requirements for consent given orally as sections 2(4)(a) to (c) do for electronic consent.

For example, under section 2(5)(a), each public body must have a formal policy or “rules” – approved by its head – outlining the specific purposes for which oral consent will be accepted. Refer to the Policy Requirements for Electronic Consent section for guidance, substituting oral consent where applicable.

Technical Requirements for Oral Consent

As per section 2(5)(d), the record of the consent must:

- Be accessible to the public body for future reference/use, and
- Be capable of being retained by the public body.

The methods by which public bodies must fulfill these requirements are not prescribed in the regulation. These methods may vary depending on the format used to record the consent, and the business needs of the public body.

The public body must authenticate the identity of the individual giving consent (section 2(5)(e)). Regardless of the authentication method used, it must be reliable for verifying the identity of the individual, and for associating the consent with the individual (section 2(5)(f)).

The reliability of the authentication method for verifying the identity of the individual giving oral consent and for associating or linking the individual with the consent will depend on the purpose for which the consent is being given. A higher degree of reliability would be required for consent to the use or disclosure of personal information considered of high sensitivity.

It is not sufficient to authenticate identity but have no means to link the individual with the information of what they consented to.

Refer to the Authentication Processes section below for more information.

Acceptable Methods for Recording Consent

Section 2(6) specifies the acceptable methods for recording oral consent:

(a) An audio recording of the consent created by or on behalf of the public body,
(b) In the form of documentation of the consent created by an independent third party, or
(c) In the form of documentation of the consent created by the public body in accordance with the rules established by the head of the public body.

Subsections (b) and (c) grant public bodies greater flexibility to determine what manner of documentation is appropriate for their business needs. However, for subsection (c), employees may only document any consent given orally in accordance with the methods and rules approved by the head of their public body.

Public bodies who choose to use subsection (c) should establish a process to ensure the documentation is being done in compliance with the established policy/rules, and the regulation.

The public body should choose the method of recording that is appropriate for the purpose for which the consent is being given, the nature of the information involved, and its business needs. In all cases, the public body must have access to, and control of the record.

Consent of a Minor

In accordance with section 2(7), a minor's consent is only valid if all applicable requirements under section 2 are met, and the public body has reasonable grounds to determine that the minor:

1. Has the capacity to understand the information relevant to providing consent (refer to Common Standards section), and
2. Understands the consequences of providing that consent.

When making this determination, the public body may consider factors such as:

- The minor's age and maturity level,
- Potential language barriers, speech impairments or cultural differences,
- Economic status/living arrangements (e.g., self-supporting or not),
- The sensitivity of the personal information in question,
- The context for the use and/or disclosure (e.g., level of impact to the minor, the purpose, etc.), and
- Whether the minor can effectively communicate their understanding.

Minors should be provided with all the information needed to understand the context and purpose for which their consent is being requested, in an age-appropriate manner, and the implications of giving, withdrawing or withholding their consent.

Exercise of Rights by a Guardian

Under section 54(1)(e) of POPA, a guardian may exercise a minor's rights and powers, in circumstances where the head of the public body determines that doing so would not be an unreasonable invasion of the personal privacy of the minor. This includes the ability to provide consent.

However, when assessing whether a guardian's exercising of this power constitutes an unreasonable invasion, the public body should also consider the minor's ability to consent for themselves.

When a guardian asserts this authority, they must provide proof of guardianship, such as a valid custody or parenting order, or other reliable evidence appropriate to the circumstances. Regardless of the evidence provided, the public body should verify the identity of the individual.

For a list of all circumstances where one individual may exercise the rights or powers of another under POPA, refer to section 54(1) of the Act.

Withdrawal and Expiry of Consent

Individuals may withdraw their consent at any time by notifying the public body.

As a best practice, public bodies should inform individuals, where possible and at the time consent is obtained, of any limitations, consequences or implications of withdrawing consent to ensure it is fully informed.

Provided all requirements are met, consent remains valid unless an individual withdraws their consent, or the expiration date of the consent, if applicable, has passed.

A public body may choose to set an expiration date for the consent, based on the circumstances and its business needs. However, even when no date is set, it is recommended that public bodies establish policies to ensure regular reviews and updates of consent after a reasonable period of time. This is a best practice measure to ensure records of consent are updated regularly, even if the consent does not expire.

Retention

While consent expiration dates are optional and the required retention period for consent records is not explicitly defined, if personal information—such as a record of consent—is used to make a decision that directly affects an individual, the public body must retain that record in accordance with section 6 of POPA and its internal retention and disposition policies.

Authentication Processes

Under section 10 of POPA, public bodies are required to protect personal information in their custody or control by making reasonable security arrangements against such risks as unauthorized use or disclosure, among others. This applies regardless of the form of consent used.

In the context of consent, privacy protection requires verifying or "authenticating" the identity of the individual giving consent. Authenticating an individual's identity can be done using a variety of methods and will likely depend on the form of consent a public body is using. Typically, these methods can be categorized into three main types:

- Something the individual knows (could include requesting confirmation of details only the individual would know such as using security questions, using multi-factor authentication, etc.).
- Something the individual has (could include requesting government-issued photo identification, or other valid identification).
- Something the individual is (could include, biometric data, such as fingerprints, voice patterns, iris scans, etc.).

As discussed under Technical Requirements for Oral Consent, the reliability of the authentication method will depend on the purpose for which the consent is being given, and the sensitivity of the personal information involved.

For consistency and to help ensure personal information is protected, public bodies should establish internal authentication processes to verify the identities of individuals.

When developing these processes, public bodies should consider various authentication methods – such as those previously outlined – based on the type and format of consent (written, electronic, or oral), how that consent is recorded, their technical capabilities, the type and sensitivity of the personal information involved, their internal information technology standards, their business needs, those of the public they serve, and their clients' technical capabilities.

Privacy Management Programs

Section 6(2)(a)(iv) of the Protection of Privacy (Ministerial) Regulation requires public bodies with a high volume of personal information, or personal information considered to be high sensitivity, to establish internal policies and procedures related to oral, electronic and written consent as part of their privacy management programs.

Each public body has the responsibility to ensure that all employees — including contractors — are informed of, and understand, these policies and procedures, as well as their specific responsibilities related to consent.