Privacy Protective Survey Guidance

March 2024

Office of the
Saskatchewan Information
and Privacy Commissioner

Privacy Protective Survey Guidance

Acknowledgement

The Saskatchewan Information and Privacy Commissioner would like to acknowledge that this resource is based on the Information and Privacy Commissioner of Ontario's *Best Practices for Protecting Individual Privacy in Conducting Survey Research* and the Alberta Government's *Conducting Surveys: A Guide to Privacy Protection*.

Purpose of This Guide

When public bodies conduct surveys involving personal information, they need to comply with Saskatchewan's access and privacy laws.

This guide raises awareness of the privacy risks that may arise when public bodies conduct surveys, including online surveys. It is not a comprehensive guide to conducting surveys. Survey project leads should consult with their Privacy Officer to ensure all privacy risks are addressed. This document is not intended to provide legal advice and is provided for informational use only.

There are separate rules and considerations that arise when a trustee as defined in *The Health Information Protection Act* (HIPA) collects personal health information as part of a survey. This guide does not consider the potential impact and specific requirements of HIPA.

Define the Purpose of Your Survey

It is important to determine the purposes of the survey project prior to developing the survey. This will help you define the information that you need to collect. Having a clear understanding of the purpose will also be key to identifying the measures that may be necessary to protect privacy and ensure compliance with *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). This is because the purpose of the study will form the guardrail for any assessments about whether there is a need-to-know personal

information. The purpose will also guide your analysis of whether any collection, use or disclosure of personal information is authorized under Saskatchewan's access and privacy laws. These considerations are discussed below.

What Privacy Laws Apply

If your survey involves personal information, the privacy rules may be found in FOIP or LA FOIP.

FOIP and LA FOIP apply to personal information in the possession or under the control of government institutions and local authorities, respectively. In this guide, those collectively will be referred to as public bodies.

FOIP and LA FOIP set out the rules that apply to the collection, retention, use, disclosure and safeguarding of personal information. These laws also include rights of individuals to obtain access to information, including their own personal information.

What is Personal Information

Section 24 of FOIP (section 23 of LA FOIP) defines "personal information" as information about "an identifiable individual" that is "personal in nature." FOIP and LA FOIP include examples of information that qualify as personal information.

Information is about "an identifiable individual" if the individual can be identified from the information, or if the information, when combined with information otherwise available, could reasonably be expected to allow the individual to be identified. Information is "personal in nature" when it reveals something personal about the identifiable individual.

Information that relates to an individual in a business, professional or official capacity may not qualify as personal information unless it reveals something personal about them. This distinction is important where a public body seeks to conduct a survey of its own workforce because the information involved may or may not qualify as personal information.

Be aware that an online survey may result in the collection of personal information that would not be collected through a paper-based survey. For example, the survey process could involve the collection of information about the respondent's internet connection. This information is called "metadata." In this context, metadata refers to information about the device or computer used by the survey respondent.

Metadata would include the Internet Protocol (IP) address used by the device. The IP address is like a street address or telephone number in that it uniquely identifies a particular device connected to the Internet.

Metadata also includes the uniform resource locater (URL) of the resource, which is an address given to a unique resource on the Web, that referred the participant to the survey. It can also include other factors, such as the time the respondent took the survey.

Metadata about computing devices can be used to facilitate tracking or monitoring of individuals, analytics, data mining and re-identification of de-identified data (*Open Government and Protecting Privacy*, (Ontario Information and Privacy Commissioner [ON IPC], March 2017). If the metadata is used in this way, it could enable the collection of other personal information.

Because metadata about devices is identifiable, Canadian privacy oversight authorities have found that it can qualify as personal information in some contexts. For example, our office has found in previous reports, such as Review Report 147-2022 and Review Report 186-2019, that an individual's IP address qualifies as their personal information pursuant to subsections 24(1)(e) and (k) of FOIP (subsection 23(1)(e) and (k) of LA FOIP).

If there is any ambiguity about whether personal information is involved, it is best to err on the side of caution and treat the information as personal information.

De-identified, Anonymous or Coded Data

De-identified Data

As noted above, information does not qualify as personal information unless an individual is identifiable from the information.

De-identification is an important tool to protect the privacy of individuals because once de-identified, a dataset does not contain personal information. If information is sufficiently de-identified, the privacy rules in FOIP and LA FOIP do not apply.

De-identified information is not defined in FOIP or LA FOIP. Information is de-identified if it does not identify an individual, and it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual.

This means that once a dataset is altered to remove any information that could be used to identify an individual, such as their name, address, birthdate, etc., then the information no longer qualifies as personal information.

Removing identifiers is important to protect privacy, but public bodies should be aware that the process of de-identification does not reduce the risk of re-identification to zero – there is always the risk of identifying someone. For more information about how to de-identify information, see the ON IPC's guidance entitled, *De-identification Guidelines for Structured Data*.

Anonymous Data

Rendering data sets anonymous requires the removal of personally identifiable information/direct identifiers and quasi-identifiable information/indirect identifiers, in such a way that individuals remain anonymous Therefore, conducting anonymous surveys is a good way to protect the privacy of the participants.

A direct identifier is information that directly identifies an individual, such as their name or driver's license number. An indirect identifier is information for which there is a "reasonable expectation" that it can be used, either alone or with other information, to identify an individual. An indirect identifier could include an individual's gender, marital status, race, ethnic origin, profession. Depending on the context, this information can be combined with other information to identify an individual. In Review Report 210-2023, our office found that a newspaper and web posting about a harassment investigation, that included the name of the municipality involved and the dates of the investigation, contained information that indirectly identified the Complainant and therefore, qualified as personal information under LA FOIP.

For these reasons, beware of the myth that surveys that do not ask for the respondent's name are anonymous. You should not assume that just because the survey does not record the participants' names that their participation is automatically anonymous. Some other examples of how an individual's identity may be revealed are:

- Where a survey provides a free text option, you will have limited control over what text is entered, and you may collect information that identifies the respondent or another individual.
- Email surveys require respondents to send their responses by email. The response will contain the email address of the sender. Where survey respondents participate in their personal capacity, in other words, not on behalf of an employer or in a business or professional capacity, their personal email address would likely qualify as their personal information.
- Third party online survey providers, and the advertisers that promote products or services on the survey providers' sites, may be able to track websites visited by the respondent by using cookies. This information can be used to develop profiles of respondents. The profiles combine information from other available

sources to provide insights into individuals. Depending on the details of the insights, these profiles may qualify as personal information.

Coded Data

An alternative is to replace all personally identifiable data in the survey with a special code. The survey data with the special code can be retained separately from the personal information. Access to the personal information through the special code should be limited to individuals with a need to know for specific, defined purposes. Survey data with this type of coding still qualifies as personal information; therefore, there is a need to comply with FOIP and LA FOIP. However, the benefit of using coded survey responses is that they limit the number of individuals who have access to the personal information.

The challenge with ensuring that respondents are not identifiable is illustrated by a privacy investigation conducted by the ON IPC, Investigation Report MC10-5. In that case, the ON IPC investigated a complaint about a paper-based survey of students conducted by an Ontario School Board. The ON IPC found that the unique survey number assigned to each paper survey linked to an identifiable student number that was maintained by the Board. Because the survey data could be linked to identifiable information, the ON IPC found that there was a reasonable expectation the individuals could be identified. Therefore, they found that the information collected through the survey qualified as personal information under Ontario's *Municipal Freedom of Information and Protection of Privacy Act*.

More recently, in our office's Investigation Report 211-2019; et al, Commissioner Kruzeniski found that a survey of teachers about their students that collected the students' initials, the name of the teacher, the grade and the school, created a "unique profile" of the students that rendered them identifiable. The Commissioner found that this information qualified as the students' personal information subject to LA FOIP.

Examine the data involved in your survey at every stage of the lifecycle to determine if it is sufficiently de-identified, truly anonymous, properly coded and/or qualifies as personal information.

Need-to-Know and Data Minimization Principles

There are two important principles that underly the privacy rules in FOIP and LA FOIP. They are the "need-to-know" principle and the "data minimization" principle.

Need-to-know requires public bodies to collect, use or disclose personal information on a need-to-know basis. This means that the personal information should only be available to those that have a legitimate need to know the information for the authorized purpose.

Data minimization requires public bodies to collect, use or disclose the least amount of personal information necessary for the purpose.

Collection of Personal Information

If your survey will involve the collection of personal information from respondents, ensure that you have the authority to collect personal information pursuant to section 25 of FOIP (section 24 of LA FOIP), which states:

> **25** No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

FOIP and LA FOIP limit the rights of public bodies to personal information so that they only collect it to the extent that it is necessary or relevant to their lawful activities. If a collection of personal information is not related to an existing program or activity, public bodies cannot rely on an individual's consent for lawful authority to collect it.

Notice of Collection

Subsection 26(2) of FOIP (section 25(2) of LA FOIP) requires a notice of collection of personal information. Public bodies must inform individuals of the purpose of the collection and any proposed uses and disclosures.

There is an exception to the requirement to provide notice in subsection 26(3) of FOIP (subsection 25(3) of LA FOIP). That provision states that notice is not required where compliance might result in "the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected."

Our office's *Guide to FOIP*, Chapter 6, at page 167 states that public bodies should rely on this exception in limited circumstances, and they should document when the provision has been used and the reasons for using it.

Although there is provision allowing for the creation of additional exceptions to this requirement by regulation, there are currently no exceptions in either *The Freedom of Information and Protection of Privacy Act Regulations*, (FOIP Regulations) and *The Location Authority Freedom of Information and Protection of Privacy Act Regulations* (LA FOIP Regulations).

Notice enables an individual to make an informed decision as to whether to provide the personal information. It also helps them understand the consequences of providing their personal information, and of exercising their privacy rights such as by making a privacy complaint. If the survey is not anonymous, individuals should be told why that is the case.

Notice should be provided at the time of collection. Notice should inform an individual of the purpose of the collection, the legal authority for the collection and the contact details for a public body employee who can answer questions.

If you contact respondents by email, whether the email is sent by you or your online survey provider, the email should include a notice about the collection, use and disclosure of personal information.

If your survey design involves a link posted on a website, provide the notice on the website.

Survey Samples

Even if your survey project will collect anonymous data from respondents, you may need to collect personal information to select the individuals who will participate in the survey. The list of participants is referred to as the "survey sample."

In addition to the names and contact details for individuals, in some cases you may need to use additional personal information. This might occur when you need a survey sample with specific characteristics such as age, gender, education or income.

You may obtain your survey sample by using names and contact details for individuals with whom your public body has had direct contact in relation to services or programs (a use of personal information). The sample may be developed from a list provided by a third party (a collection of personal information). You may decide to ask another public

body to use personal information it possesses to develop a sample and contact individuals on your behalf. Each of these raises different privacy issues that are addressed below.

Survey Sample is Taken From Your Public Body's Clients

If you intend to use personal information in your possession to create your survey sample, ensure compliance with section 28 of FOIP (section 27 of LA FOIP) which prohibits the use of personal information without consent unless certain conditions are met.

If you do not have consent, determine if your sampling of survey participants is a use of personal information for purposes consistent with the reason it was collected.

"Consistent purpose" is defined as one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses the personal information.

"Consent" should be thought of as a process that provides the individual with a measure of control over their own personal information. It means a voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another; it supposes a physical power to act, a moral power of acting and a serious, determined and free use of these powers.

To rely on a consent, ensure that it complies with the FOIP Regulations, section 18 and, where applicable, the LA FOIP Regulations, section 11.

Further information about obtaining consent can be found in our office's *Best Practices for Gathering Informed Consent*.

Survey Sample is Provided by Another Public Body

If your plan is to collect personal information from another public body to create a survey sample, consider the requirements of section 25 of FOIP (section 24 of LA FOIP) which, as noted above, governs the right to collect personal information.

Be aware that the collection of personal information from another public body is an "indirect collection" of personal information.

Section 26 of FOIP (section 25 of LA FOIP) requires public bodies to collect personal information where reasonably practicable directly from the individual to whom the information relates unless the listed exceptions apply.

Exceptions include where the individual authorized a collection by other methods, if the information may be disclosed to your public body pursuant to subsection 29(2) of FOIP (subsection 28(2) of LA FOIP), and if the information is collected for the purpose of management or administration of personnel.

In this scenario, you will need to ensure that the public body disclosing the information has the authority to do so. Section 29 of FOIP (section 28 LA FOIP) prohibits the disclosure of personal information without consent except in accordance with that section or section 30 of FOIP (section 29 of LA FOIP).

Subsection 29(2)(k) of FOIP (subsection 28(2)(k) of LA FOIP) may also be relevant. It enables disclosure to any person or body for research or statistical purposes if certain conditions are met.

Note that "research" and "statistics" are not defined in FOIP or LA FOIP. My office's *Guide to FOIP*, Chapter 6, at pages 227-228, sets out the following definitions:

> "Research" means the systematic investigation into and study of materials, sources, etc., to establish facts and reach new conclusions. For a disclosure of personal information for "research purposes" to be permissible, the researcher must intend to use the personal information to investigate and ascertain facts or verify theories.
>
> "Statistics" is the science of collecting and analyzing numerical data, especially large quantities of data and usually inferring proportions in a whole from proportions in a representative sample, any systematic collection or presentation of such facts. In this context, quantifiable personal information to study trends and draw conclusions.

Subsection 29(2)(k)(ii) of FOIP (subsection 28(2)(k)(ii) of LA FOIP) requires that public bodies who share personal information for these purposes have a written agreement with the receiving public body to clarify the rights and obligations of each party with respect to the information. Any written agreement should also specify the authority each party is relying on for the collection or disclosure of the personal information in question. The agreement will help to ensure compliance with FOIP and LA FOIP.

If your public body is a government institution under FOIP and the purpose of your survey relates to a "common integrated service," section 17.1 of the FOIP Regulations may permit the disclosure of the personal information for your survey sample." A "common integrated service" is defined in subsection 17.1(1)(a) of the FOIP Regulations as a program or activity designed to benefit health, safety, welfare or social well-being of an individual that is delivered by a government institution and entity including, another government institution, a local authority, a trustee as defined in HIPA. You will need to

enter into an information sharing agreement with the other entity. The requirements for the information sharing agreement are set out in subsection 17.1(2) of the FOIP Regulations.

Another Public Body Administers the Survey

Your plan may be to ask another public body to use personal information from its own data sources to identify a survey sample, contact participants, and carry out the survey on your behalf. If you select this option, then the public body conducting the survey must have the authority to use the personal information for this purpose. If your public body and the other public body have a direct interest in the subject of the survey and its results, the use may be authorized as a consistent use.

Third Party Survey Providers

Regardless of who conducts your survey, the same privacy rules apply to any personal information collected. If you retain the services of a third party, such as a survey company, online survey provider or another public body to do the research, a written agreement is needed to ensure that the other party complies with FOIP and LA FOIP.

Subsection 2(1)(b.1) of FOIP defines "employee of a government institution" as an individual employed by a government institution and includes an individual retained under a contract to perform services for the government institution. There is a corresponding definition in LA FOIP. You will need to consider if the entity retained to conduct the survey qualifies as an "employee" of your public body.

In the privacy world, when personal information is provided to a contractor to facilitate the provision of a service, this constitutes a "use" and not a "disclosure." Therefore, when a public body transfers information for processing, it can only be used for the purposes for which the information was originally collected.

Contracts with online survey providers raise some additional privacy concerns that must be addressed.

Ensure that your online survey provider does not allow third parties to track participants. This might arise where an online survey provider permits advertisements and social media analytics to gain access to data. As noted above, information gathered from survey participants could be used with other information to identify individuals.

Therefore, you should not use an online survey provider that allows third parties to track survey participants.

Many online survey providers offer their services under non-negotiable terms of service and privacy policies. It is your responsibility to ensure that the provider's terms of service agreement and privacy policy allow for the secure collection, retention, use, disclosure, security and disposal of personal information in accordance with FOIP and LA FOIP.

For example, consider how the terms of service address the following:

- Data ownership (possession or control)
- Prohibitions against selling, sharing or disclosing the data
- Controls on use of data by the provider's staff
- Measures to protect individuals right of access to their own personal information
- Account and data deletion and destruction
- Safeguards
- Privacy breach response

Online survey providers may update or change their terms of service and privacy policies. In some cases, the online survey provider may be entitled to change the terms of service without notice to you.

Survey data may be stored outside Canada depending on the location of the online survey provider's servers. Storing data outside Canada may make it subject to the laws of that jurisdiction. There is no prohibition against the storage of data outside Canada. However, you will need to ensure that storage of the data outside Canada is not contrary to your public body's policies and does not put the data unnecessarily at risk. You should also ensure that individuals are notified that their data will be stored outside Canada and that reasonable measures are in place to protect privacy and security of the information. This will require you to assess the risk of storage outside Canada.

Information Management Service Providers

If you are using a third-party service to conduct the survey, consider if it qualifies as an information management service provider (IMSP) under FOIP or LA FOIP. Subsection 2(1)(e.1) of FOIP (subsection 2(1)(e.1) of LA FOIP) defines information management service providers as a person or body that processes or provides information management or information technology services to a government institution or local authority with respect to the record.

Section 24.2 of FOIP (23.2 of LA FOIP) permits public bodies to provide personal information to an IMSP for the purposes of having the IMSP process the information or enabling the provision of technology services. Subsection 24.2(2) of FOIP (subsection 23.2(2) of LA FOIP) requires that public bodies enter into a written agreement with the service provider that governs the access to and use, protection of the personal information and meets the requirements of the acts. Additional requirements for the agreements are set out in section 13.1 of the FOIP Regulations (section 8.2 of the LA FOIP Regulations).

Pursuant to subsection 24.2(4) of FOIP (subsection 23.2(4) of LA FOIP), an IMSP is required to comply with the terms and conditions of the agreement. Therefore, if your survey provider qualifies as an IMSP, you will need to ensure that the terms of service comply with this provision.

Self-Hosting an Online Survey

There are some software programs or applications that are available if you want to host your own online survey. Hosting your own survey will mitigate the risks of using a third party. It will also avoid the risks that arise when data is stored outside Canada.

If you decide to host the online survey yourself, consult technical experts to ensure that the application you use to conduct the survey will operate in a way you expect it to and that it does not collect, use or disclose personal information in a manner that is not planned.

Safeguards

Public bodies have a duty to protect personal information. This requirement is set out in section 24.1 of FOIP (section 23.1 of LA FOIP). It includes requirements to protect the integrity, accuracy and confidentiality of personal information. It also includes requirements to protect against any reasonably anticipated loss of personal information and unauthorized use, disclosure or modification.

Public bodies must then establish administrative, technical and physical safeguards to protect personal information. For example, survey results containing information about identifiable individuals must be stored in a secure location. If you plan to store any personal information collected as part of your survey on mobile devices such as a laptop,

phone or USB key, encryption is essential. Ensure that the data is encrypted in transit. If you are storing large volumes of personal information on network drives, encryption is highly recommended.

If public bodies are using a third party to host their online survey, they will need to be satisfied that the third party has these safeguards in place and that the requirements for the safeguards are set out in a written contract or terms of service.

Use and Disclosure of Survey Results

Survey results should be reported in a way that protects the privacy of the respondents. This means that personal information collected in surveys must only be used for the purpose it was collected and should only be reported in an aggregated, non-identifying manner.

Take steps to ensure that the results do not include small cells of information that could be used to re-identify individuals. For example, in an anonymous survey of your employees, the results might include information about gender and employee job classification (e.g., executive, manager, supervisor or staff). If there is only one individual of a particular gender who falls within a job classification, then that individual's responses will be identifiable. It may be possible to transform any survey results that are identifiable in a way that protects personal information such as by de-identifying or re-coding the information.

Privacy Impact Assessment

You should do a preliminary assessment to determine if personal information is involved at the survey sampling and survey stage of the project. The preliminary assessment will also help you decide what privacy laws apply.

Once you have determined that personal information is involved and which of Saskatchewan's privacy laws apply, you should conduct a Privacy Impact Assessment (PIA).

A PIA is a process that assists organizations in assessing whether a project, program or process complies with the applicable access and privacy legislation. When a project, program, process is in the design stage, a PIA should be used to identify areas where there may be a "privacy impact." A "privacy impact" occurs when there are inadequate

safeguards to protect personal information. They also occur when there is a collection, use, and/or disclosure of personal information that is not authorized by privacy laws.

As set out in our office's *Privacy Impact Assessment Guidance*, when a PIA is conducted, that is an opportunity for organizations to make adjustments to the project, program or process to ensure personal information is protected to the greatest extent possible and all practices comply with the applicable laws. Consult your Privacy Officer to see if your organization has developed its own guidance or policy on how to conduct a PIA.

Other Considerations

Consider if your survey requires research ethics board (REB) approval. Your survey may require REB approval if your survey qualifies as "research" involving "human participants." Both terms are defined in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*. For more information about the need for REB approval, consult your Privacy Officer and the Tri-Council Policy Statement.

Organizations and individuals may seek access to the personal information and other information involved in the survey. Individuals may seek access to or correction of their own personal information. Public bodies will need to consider how they will provide individuals with their right to access or correction while protecting the personal information of other individuals. You may also be required to respond to a complaint about a privacy breach and will need to have policies in place to ensure appropriate breach response.

Contact Information

If you have any questions or concerns about these guidelines, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC