

# Fact Sheet: Disclosures of Non-Personal Data

This fact sheet provides information about disclosures of non-personal data under the *Protection of Privacy Act* (POPA).

## What is “non-personal”?

Section 1(n) of the POPA defines non-personal data to mean data, including data derived from personal information (refer to Fact Sheet: Data Matching and Data Derived from Personal Information), that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the regulations.

## Disclosure of non-personal data to a public body

Section 23(1)(a) authorizes the disclosure of non-personal data between public bodies. There are no limits on when a public body can disclose non-personal data to another public body.

## Disclosure of non-personal data to a person other than a public body

Section 23(1)(b) sets the parameters when a public body wishes to disclose non-personal data to a person or organization that is NOT a public body.

This includes requirements related to the purpose for the disclosure and conditions that must be approved by the head prior to a disclosure happening.

### Purpose of disclosure

A public body is only authorized to disclose non-personal for the following reasons:

#### Research and analysis

*Research* means for the purpose of the systematic investigation and analysis or study of materials or sources in order to establish facts or to verify theories.

*Analysis* refers to the process of examining and interpreting collected information to identify patterns, relationships, and trends. It often involves breaking data down into smaller parts, comparing findings, and drawing conclusions.

The disclosure of non-personal data for research and analysis purpose is to ensure public bodies can use data to make accurate and informed decisions without putting individuals' personal privacy at risk.

#### Planning, administering, delivering, managing, monitoring or evaluating a program or service

*Planning* means to think about and decide what to do or how to do something.

*Administering* means to control the operation or arrangement of something.

*Delivering* means to provide a service.

*Managing* means to be responsible for controlling or organizing something.

*Monitoring* means to watch and check something carefully over a period of time.

*Evaluating* means to judge or calculate the quality, importance, amount, or value of something.

#### One or more prescribed purposes

A prescribed purpose is one that is allowed through regulation, however, at this time there are no prescribed reasons for which a public body can disclose non-personal data.

A public body can disclose non-personal data to a third party to prepare and review current and proposed programs or services, including common or integrated programs or services

### Approved Conditions

The head of a public body must approve conditions related to security and confidentiality, limitations on re-identifications and subsequent use or disclosure, as well as conditions related to the destruction of the data.

Any signed agreement should include compliance provisions related to the required conditions specific to the project, the POPA and its regulations, and any related policies and procedures of the public body disclosing the data should consider relevant.

Any agreement between the public body and the other party should meet the conditions listed below.

#### Security and confidentiality

*Security* refers to protecting or guarding the non-personal data provided to a person or organization that is not a public body from unauthorized access, use, disclosure, theft or other danger.

*Confidentiality* refers to the condition whereby non-personal data is kept private and safe from unauthorized access, use or disclosure. It means that there is no disclosure, orally or otherwise, other than to those working on the project.

Examples of security and confidentiality requirements that should be considered for including:

- the names of the individuals who will be given access to the data must be provided;
- an agreement to adhere to the same conditions contained within the agreement with the public body;
- acknowledgement that the data must be kept in a secure location;
- security classifications applied to the data;
- administrative, technical and physical safeguards used to protect the non-personal data.
- any audit provisions so that the security confidentiality measures employed by the person or organization that is not a public body can be reviewed;
- clauses related to failure to meet the conditions may result in cancellation of the agreement and leave the person or organization open to charges under section 60(1) of the Act.

#### Prohibition re-identification of the non-personal data

Any agreement should indicate the prohibition of any actual or attempted re-identification of the non-personal data. This ensures the protection of privacy for individuals whose information has been modified or anonymized.

#### Prohibition of any subsequent use or disclosure

Non-personal data cannot be used or disclosed beyond the original purpose without the express authorization of the public body.

The prohibition includes a ban on the sale or giving of the data for any purpose.

Under 23(2), the public body can only give express authorization to subsequently use or disclose non-personal data under certain circumstances. They may authorize it:

- if it is for the one of the permitted purposes under the Act,
- if the head of the public body approves any additional conditions, relating to the subsequent use or disclosure, and
- if there is a revised or new signed agreement, that applies to the subsequent use or disclosure.

Note: a separate agreement with all the required compliance conditions must be signed by the prior to further using or disclosing the data for the additional purpose.

#### Destruction and retention

When non-personal data is shared under section 23(1) and the non-personal data has served its purpose, it should be destroyed at the earliest reasonable time. The only exception is if the head of the public body has given authorization under 23(1)(ii)(C) and a new agreement has been signed

#### **Exceptions to disclosures**

Section 23(3) clarifies that POPIA is not meant to restrict the disclosure of a report, summary or other publication containing non-personal data that is in aggregate or statistical form.

*Aggregate or statistical form* means combining personal information or data derived from personal information collected from several sources into a single data set, summarizing it and transforming it into non-personal data.

The intent of 23(3) is to allow for these types of disclosures.

Additionally, non-personal data cannot be disclosed under a formal access the information request under the *Access to Information Act*.