Fact sheet: Creation and Use of Non-Personal Data

The *Protection of Privacy Act* (POPA) allows public bodies to create and use non-personal data.

What is "non-personal data"?

Section 1(n) of the Act defines non-personal data to mean data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the regulations.

Authorized purposes

Section 21(1) authorizes the creation of non-personal data for one or more listed purposes. If authority does not exist under this provision, a public body cannot create non-personal data. A public body can only create non-personal data from personal information or data derived from personal information if it is already in its custody or control.

Research and analysis
Research means for the purpose of 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 creation of non-personal data for research and analysis is to ensure public bodies can modify, anonymize or generate non-personal data from personal information 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 create non-personal data.

Data quality assurance process

When creating non-personal data, section 5(1) of the Protection of Privacy (Ministerial) Regulation requires that a public body must establish a data quality assurance process to:

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

Creation of non-personal data

Under 21(3), for the purposes of creating non-personal data, a public body may only use personal information or data derived from personal information if it is already in the custody or under the control of the public body. Meaning a public body cannot collect personal information from another public body to create non-personal data unless it is an authorized collection.

Non-personal data created must be created in accordance with:

Generally accepted best practices
These are widely recognized methods, techniques, or guidelines that are considered the most effective or efficient in a particular field. These practices are often developed through experience, research, and expert consensus, and they help ensure consistency, quality, and success in various industries or professions.

When it comes to the creation of non-personal data public bodies should be ensuring that information is

modified, generated or anonymized in accordance with industry standards.

Prescribed requirements

Public bodies may only create non-personal data in accordance with the regulations. Section 5(1) of the Protection of Privacy (Ministerial) Regulation requires that a public body must establish a data quality assurance process when creating non-personal data to:

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

Creation of non-personal data record

In order to create non-personal data, a public body is required to use appropriate measures to ensure that the personal information or data that is used to create it is protected.

A public body must maintain a record in accordance with any prescribed requirements of the description of the personal information or data to be used, the purpose for the creation, the method used to de-identify the personal information or data and the steps taken/assessment done to ensure that the identity of any individuals who are the subject of the non-personal data cannot be identified or re-identified from the data.

When using higher sensitive personal information or data, this information should be included in a privacy impact assessment.

As a best practice, a public body should implement a policy that outlines its processes when considering whether to create non-personal data featuring such considerations as whose approval is required, what assessment tools and technical methods will be required, etc.

Use of non-personal data

Section 22 allows a public body to use non-personal data created under section 21(1) for any purpose. Unlike personal information and data derived from personal information, there are no restrictions on a public body's use of the non-personal data it has created.

However, before a public body uses or discloses non-personal data, section 5(2) of the Protection of Privacy (Ministerial) Regulation requires a public body to conduct an assessment that ensures, to the extent possible, that the identity of any individual who is the subject of the non-personal data cannot be identified or reidentified from the data, that identifies the security classification level of the created non-personal data, and that identifies the level of risk of reidentification and security measures taken to reduce the risk.

Protection of non-personal data

The head of the public body must protect non-personal data by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. However, this obligation extends to all public body employees, as defined in section 1(h) of the POPA.

- *Reasonable* means based on good judgement and therefore fair and practical.

As with a privacy management program, a public body must implement policies or procedures on use of non-personal data within a public body. These policies or procedures may include:

- Implementing strong access controls by limiting employee access to personal information or data derived from personal information when creating non-personal data to need to know only
- Using multi-factor authentication wherever possible to add an extra layer of security
- Employ strong and unique passwords
- Use encryption for sensitive data that is both at rest and in transit to ensure that even if it is compromised, it remains unreadable and unusable without the encryption keys
- Regularly reviewing the procedures used to create non-personal data (e.g., methods used, forms, approvals, etc.) to ensure they are adequate and up to date
- Requiring privacy impact assessments on projects that involve the creation of non-personal data
- Regularly reviewing security measures to ensure they are adequate by performing internal and external security assessments, penetration testing, and vulnerability scanning to help identify potential weaknesses and areas for improvement
- Having a privacy incident procedure in place
- Having processes in place to document the creation of non-personal data

- Having information management policies in place to securely store and destroy non-personal data
- Requiring employees complete regular training related to their privacy protection obligations
- Developing a comprehensive cybersecurity strategy that outlines the approach to cybersecurity, including risk assessment, incident response, employee training, and ongoing monitoring
- Regularly updating software and systems as outdated software can be vulnerable to security flaws
- Regularly backing up data to help mitigate the impact of data loss due to cyberattacks, hardware failures, or natural disasters
- Dividing the network into separate segments to limit the potential impact of a security breach by restricting lateral movement by attackers and helps contain any compromised systems

Implementing policies shows a public body is taking its obligation to protect non-personal data seriously and will strengthen its compliance with regards to Privacy Management Programs, refer to the Fact Sheet: Privacy Management Programs.

Public bodies must also ensure that contractors follow proper policies or procedures. When contracting for services involving the creation of non-personal data, public bodies should incorporate privacy protection provisions in the contract.

Additional resources

Cybersecurity Best Practices

Fact Sheet: Privacy Management Programs