Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing Privacy Code factsheet 6

Storage, security, retention and disposal – Rule 5 and Rule 9

This factsheet covers:

- Rule 5: Storage and security
- Rule 9: Retention and disposal

This factsheet provides a summary of our guidance on rules 5 and 9. See the full guidance for more detailed information.

Rule 5: storage and security

Organisations must have effective security safeguards that protect against **loss**, **unauthorised access, use, modification or disclosure** of people's biometric information.

What are security safeguards?

Security safeguards enhance the level of protection for people's biometric information. Different safeguards will offer different protections. It's important to layer multiple safeguards to ensure there are many layers of protection for information. Safeguards need to reflect the sensitivity of the biometric information an organisation holds, as well as the overall risk based on the handling of that information.

Some examples of key security safeguards when developing an organisation's security plan are technical security controls (e.g. encryption of biometric information, applying security fixes and updates), organisational security controls (e.g. staff training, policies, audits) and physical security controls (e.g. locked rooms).

Organisations must have processes in place for if a privacy breach or security incident occurs. See our guidance on breach management which applies to biometric information.

Rule 9: retention and disposal

Another protection of people's biometric information is not holding onto it for longer than needed.

When do organisations need to get rid of biometric information?

Organisations need to dispose of biometric information when it is no longer necessary to hold it for the purpose for which the information may lawfully be used.

If an organisation doesn't have a lawful purpose for keeping biometric information, it must be disposed of securely, whether it's in physical or digital form. Disposing information means it should no longer be retrievable.

Third-party providers

If an organisation is using a third-party provider, it's important to have oversight of the third-party's storage, security, retention and disposal policies and safeguards.

A 'third-party provider' means an external provider that an organisation is using to store or process biometric information on its behalf or for another service. For example, an organisation may use a third-party provider for identity verification services that uses facial and voice biometrics.

We have guidance on obligations when using third-party providers which also applies to biometric information.

Where to go for more information

- Biometrics guidance on rule 5 and rule 9
- Security safeguards in rule 1 guidance

- Security and Internal Access controls Poupou Matatapu guidance
- Know your personal information Poupou Matatapu guidance
- Measure and monitor Poupou Matatapu guidance
- Third party providers
- Cert NZ's Critical Controls
- New Zealand Information Security Manual (NZISM)