Privacy Commissioner
Te Mana Mātāpono Matatapu

# Biometric Processing Privacy Code factsheet 2

## Collection of biometric information – rules 1-4

This factsheet covers:

- Rule 1: Purpose of collection
- Rule 2: Source of biometric sample
- Rule 3: Collection of information from individual
- Rule 4: Manner of collection of biometric information

This factsheet provides a summary of our guidance on rules 1-4. See the full guidance for more information.

## Rule 1: Purpose

Rule 1 is about your purpose for collecting biometric information.

Organisations must only collect biometric information if they can meet all the below conditions:

1. The collection is for a lawful purpose.
2. The collection is necessary. Necessary includes that it is effective and there are no reasonable alternatives with less privacy risk.
3. It has implemented appropriate privacy safeguards.
4. The biometric processing is proportionate to the likely impacts on people.

### 1. Lawful purpose

The lawful purpose is what an organisation wants to use biometrics for.

The purpose must be specific, relevant and connected to the functions and activities of the organisation.

## 2. Necessary for a lawful purpose

Biometric information may only be collected if the biometric processing is **necessary** for the purpose.

The collection of the specific biometric information must be **needed** to fulfil the organisation's purpose and be relevant and not excessive. Necessary also means that the biometric processing is **effective** and there is no reasonable and effective alternative with less privacy risk that the organisation could use instead.

### Effective

Effectiveness is the degree to which the biometric processing directly enables the organisation to achieve its purpose. Organisations can use a range of different evidence to assess effectiveness – for example, performance metrics from biometrics vendors or independent assessors, or by reviewing data from tests or trials.

### Is there an alternative option with less privacy risk?

If an organisation could achieve its purpose as effectively through an alternative means with less privacy risk, then the biometric processing will not be necessary.

An alternative means could be non-biometric processing, or it could be a different type of biometric processing that has less privacy risk. For example, depending on the purpose, a non-biometric alternative to biometric processing could be a quality CCTV system, using security guards, offering an access card, or a manual sign in or identity verification.

The alternative does not need to achieve the exact same outcome as the biometric processing for it to be a reasonable alternative.

### Running a trial

In some situations, an organisation may establish a trial to assess whether its proposed use of biometrics for a particular purpose is going to be effective, and therefore necessary to achieve its purpose. Organisations can also use evidence gathered from the trial to assess whether there is a reasonable and effective alternative with less privacy risk. Running a trial only allows compliance with the necessity test to be deferred until the end of the trial period. During the trial, organisations must comply with all other parts of the Code except the necessity test.

Trials can only run for a limited time and organisations must tell people that they are running a trial.

## Privacy safeguards

Privacy safeguards are things that reduce privacy risk, e.g. having human oversight of a biometric system, deleting biometric samples (if appropriate), or implementing security protections for biometric information.

Organisations need to put in place reasonable privacy safeguards **before** collecting biometric information.

## 3. Proportionality

Organisations must not collect biometric information unless the biometric processing is proportionate to the likely impacts on people. To assess whether the biometric processing is proportionate, organisations need to assess:

- The scope, extent and degree of **privacy risk** from the biometric processing.
- Whether the **benefit** of achieving the lawful purpose through the biometric processing outweighs the privacy risk.
- The **cultural impacts and effects** of biometric processing on Māori.

### Assess privacy risk

Organisations must assess the degree of privacy risk from the use of biometrics.

Privacy risk is any reasonable likelihood that the privacy of individuals may be infringed by the biometric processing. It includes a range of actual or potential impacts on people, including risks related to inaccuracies, security vulnerabilities, bias, discrimination and any other infringements on an individual's privacy interests or legal rights and freedoms.

When considering privacy risk, organisations should consider both how likely it is an event will occur, and what the consequences would be if an event occurred.

The volume and nature of the information, whose information it is, who collects it, why it is collected, and the context and design of the biometric system are all factors that impact the degree of privacy risk.

### Benefit

Organisations need to assess the benefit of achieving their purpose through biometrics. The benefit could be a public benefit, a benefit to the people whose information is being collected, or a benefit to the organisation collecting the information. Then organisations need to weigh the benefit against the privacy risk.

The benefit must outweigh the privacy risk. If an identified benefit is to the organisation collecting the information, the benefit must outweigh any privacy risk by a substantial degree to be proportionate.

### Cultural impacts and effects on Māori

The last part of the proportionality assessment is taking into account the cultural impacts and effects on Māori.

Cultural impacts and effects could result from:

- cultural perspectives that affect how Māori view or are impacted by biometric processing (e.g. tikanga Māori, Māori data sovereignty),

- any different impact the processing has on Māori (e.g. discrimination due to bias in the system).

We encourage you to read the full guidance in rule 1 on cultural impacts and effects on Māori.

## Rule 2: collect biometric samples directly from the person

Rule 2 requires that organisations only collect biometric samples directly from the person whose information it is, unless an exception applies. Some exceptions are if the individual authorises the organisation to collect it from someone else, or if collecting it from someone else is necessary to prevent or lessen a serious threat to someone's life or health.

Some examples of direct collection are:

- An organisation uses a camera to take images to enrol people in a facial recognition system.
- An organisation uses a scanner to take a fingerprint sample from someone to use in a security access system.
- An organisation collects a voice sample from a customer when they call the call centre for fraud detection and prevention purposes.

## Rule 3: tell people about the information you collect

Organisations are required to be transparent, so people know about their use of biometrics.

### The minimum notification rule: what to tell people before or at the time their information is collected

Organisations must tell people the following information **before** or **at the time** their biometric information is collected:

- The fact that the biometric information is being collected.
- Each purpose for which the biometric information is being collected.
- Whether there is any alternative option to biometric processing that is available.

This information must be communicated in a **clear and conspicuous** way. Organisations must also include a location, address or other method for people to obtain further information about the biometric processing.

### Other information that must be notified

Rule 3 also requires organisations to tell people other more detailed information before collecting their biometric information, or if that is not practicable, as soon as practicable after collecting their biometric information. For example, organisations must tell people that they have a right to access and correct their biometric information.

The rule 3 guidance provides more about the transparency rules and the limited exceptions to the notification requirements.

## Rule 4: be fair in how you collect biometric information

Rule 4 is about **how** organisations collect biometric information. When collecting biometric information, organisations must not breach the law or collect information in an unfair or unreasonably intrusive way. Special care must be taken when collecting information from children and young people.

### Where to go for more information

- Biometrics guidance for rule 1, rule 2, rule 3 and rule 4
- Collecting personal information guidance
- Know your personal information Poupou Matatapu guidance
- Assessing risk Poupou Matatapu guidance