# Biometric Processing Privacy Code factsheet 3

## Use of biometric information – Rules 10, 8, and 13

This factsheet covers:

- Rule 10: the limits on using biometric information
- Rule 8: accuracy of biometric information
- Rule 13: unique identifiers

This factsheet provides a summary of our guidance on rules 10, 8 and 13. See the full guidance for more detailed information.

## Rule 10: limits on use of biometric information

Rule 10 is about the limits on what an organisation can use biometric information for.

### General limits on use of biometric information

The general rule is that organisations can **only use biometric information for the purpose they collected it for,** unless an exception applies. For example, if the new purpose is directly related to the original purpose that the organisation collected the information for.

### Limits on biometric categorisation

In addition to the general use limits, rule 10 contains limits on using someone's biometric information to infer or detect certain sensitive information about them unless an exception applies (also referred to as biometric categorisation or inferential biometrics). In general, an organisation must not use biometric information for biometric categorisation unless an exception applies.

For example, an organisation must not use someone's biometric information to detect:

- A person's health information, unless the person specifically authorises the organisation to do so.
- A person's state of fatigue, unless doing so is necessary to avoid endangering someone's life, health or safety.

## Rule 8: accuracy of biometric information

Rule 8 is about ensuring that organisations take reasonable steps to ensure biometric information is **accurate**, up to date, complete, relevant and not misleading before it is used in biometric processing or disclosed.

An organisation's biometric system needs to be sufficiently accurate for the overall context, privacy risk and people whose information it is collecting.

In most cases, this means an organisation's system needs to be accurate in the vast majority of cases (i.e. it is highly accurate). If an organisation operates a system that is not very accurate, it will be hard to show that it is effective (therefore, you may also be in breach of rule 1).

## Rule 13: unique identifiers

A **unique identifier** is a number, symbol or other particular that an agency can use to uniquely identify a person in their system (other than the person's name). Examples of non-biometric unique identifiers are IRD numbers or National Health Index (NHI) numbers. It is possible for an organisation to assign a biometric template as a unique identifier.

The Code contains some technical restrictions on the use of unique identifiers that can apply to biometric information.
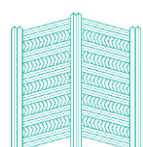
## Where to go for more information

- Biometrics guidance for rule 10, rule 8, and rule 13
- [When can I use the directly related purpose exception](#) AskUs question
- [Using and disclosing personal information](#) guidance