Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing Privacy Code factsheet 1

Overview

Biometric Processing Privacy Code 2025

The Code regulates how organisations collect, hold, and use **biometric information** for the purposes of **biometric processing**. We use the term biometrics to mean when technologies like facial recognition are used to collect and process people's biometric information to identify or classify them.

This factsheet provides a general overview of what the Code applies to. The factsheet is a summary of our full biometrics guidance. See the full guidance for more detailed information.

Who does the Code apply to?

The Code applies to organisations who collect people's biometric information in an automated process to verify, identify or categorise them i.e. carry out biometric processing.

Note:

- If the organisation is a health agency and carries out biometric processing to provide someone with health services, the Code won't apply (they are covered by the Health Information Privacy Code instead).
- Some specific rules do not apply to the New Zealand Security Intelligence Service and the Government Communications Security Bureau.
- The Code generally does not apply to personal consumer devices like smartwatches, fitness trackers, or VR headsets.

- The Code generally does not apply obligations to individual people in their personal capacity, unless there is very high risk.

What information and activities are regulated?

An organisation must comply with the rules in the Code when they use **biometric information** in automated **biometric process**.

Biometric information

Biometric information is information about how someone looks, moves or behaves. For example:

- Physical features of a person e.g. their face, fingerprints, or iris.
- How a person typically acts with their body e.g. how a person walks, sounds when they speak, writes or types.

But it doesn't include any biological or genetic material (e.g. blood or DNA), or information about a person's brain activity or nervous system.

Biometric information can be in digital or analogue records, like a photo or scan (biometric samples), or in algorithmic formats (biometric templates). Both are regulated by the Code.

Biometric processing

The Code applies when an organisation collects and processes someone's biometric information to:

- **Verify** their identity – one-to-one matching (biometric verification).
- **Identify** them out of a group or database of people – one-to-many matching (biometric identification).
- **Categorise** them or infer other information about them (biometric categorisation). For instance, using a biometric system to infer someone's emotions from their voice or estimate their age from their face.

Key concepts in the Code

Some of the key concepts in the Code are:

- **Purpose:** An organisation needs to know **why** it is collecting biometric information and only collect the information that it needs for that purpose. The collection must be necessary and effective for that purpose.
- **Safeguards:** Organisations need to implement privacy safeguards before collecting biometric information. Privacy safeguards are measures that reduce privacy risk, ensure transparency and accuracy of the biometric system, and increase the security controls for biometric information.
- **Proportionality:** An organisation must not collect biometric information unless it believes on reasonable grounds that the biometric processing is proportionate to the likely impacts on people.
- **Openness:** Organisations generally need to let people know how their biometric information is going to be used and disclosed so they can make decisions about whether to provide it.
- **Use limits:** The Code sets limits on what organisations can use biometric information for. For example, organisations may not use a person's biometric information to detect that person's health information unless the person specifically authorises it.

The Code's 13 rules

The 13 privacy rules of the Code substitute for the 13 privacy principles of the Privacy Act.

From the point of view of an organisation, the rules in the Code can be summarised:

1. Only collect biometric information if it's necessary, effective and proportionate and with the right safeguards in place.
2. Get it straight from the people concerned where possible.

3. Tell them why you're collecting biometric information, and if there's an alternative option.
4. Be fair when you're getting it.
5. Take care of it once you've got it.
6. People can ask if you have their biometric information and see their biometric information if they want to.
7. They can correct it if it's wrong.
8. Make sure biometric information is correct before you use it.
9. Get rid of it once you're done with it.
10. Use it for the purpose you got it and don't categorise people unless there is a good reason.
11. Only disclose it if you have a good reason.
12. Make sure that biometric information sent overseas is adequately protected.
13. Only assign unique identifiers if permitted.

The other factsheets in this series have more detailed information on the rules.

How the rules are enforced

The first stop for a complaint will always be the organisation itself. Organisations must have privacy officers and should have complaint handling procedures.

OPC will take compliance action in relation to the Code in line with our Compliance and Regulatory Action Framework.

Where to get additional assistance

There are five other Biometric Processing Privacy Code factsheets that give a broad overview of how the Code works in practice.

We also have a full set of guidance on each rule in the Code with worked examples on our website. We also have an AskUs knowledge base of frequently asked questions.

If you think an organisation isn't complying with the Code, you should raise your concerns directly with them before you make a complaint to us. Read about making a complaint.