Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing Privacy Code draft guide – introduction and overview

Privacy Commissioner
Te Mana Mātāpono Matatapu

Contents

Introduction to the Code

This document contains guidance on the draft Biometric Processing Privacy Code (the Code) that is being issued for consultation under s 33 of the Privacy Act. This guidance is to help organisations and individuals understand the code and how it could apply to them.

If the Privacy Commissioner decides to issue a Biometric Processing Privacy Code following the consultation on the code, the Office of the Privacy Commissioner (OPC, we) will continue to revise this guidance and will publish further guidance at a later date.

We especially welcome feedback on the guidance during the consultation period for the Code (17 December 2024 – 14 March 2025), but we are also always open to feedback on our guidance. You can send any feedback on the draft guidance to biometrics@privacy.org.nz. You can include feedback on both the guidance and the Code or provide feedback separately. We invite feedback on the whole guidance, or on a particular section.

What does the Code apply to?

The Code applies to **biometric information** as a class of information and to the activity of **biometric processing**.

Biometric information

Biometric information is information about a biometric characteristic, which is used for the purpose of biometric processing. Biometric characteristic includes:

- Physical features of a person e.g. their face, fingerprints, or iris.
- Information about how a person typically acts with their body, e.g. how a person walks, writes or types.
- A combination of physical features and how a person typically acts, e.g. how an individual sounds when they speak.

Biometric information also includes:

- A **biometric sample**, which is a record (either physical or digital) of an individual's biometric characteristic e.g. a photo of a face, a scan of a fingerprint or a video of someone's gait when they walk.
- A **biometric feature**, which is a representation of information extracted from a biometric sample e.g. how an algorithm recognises the information in a biometric sample.
- A **biometric template**, which is a stored set of biometric features.

Biometric information does **not** include any information about an individual's biological or genetic material (e.g. blood or DNA), brain activity or nervous system.

Examples of biometric information under the code	Not biometric information under the code
A photograph of someone's face that is being used in a facial recognition system (also called FRT).	A photograph of someone's face which you are using in an internal newsletter.
Footage of someone walking that will be analysed by a biometric system to identify the person by their gait.	Footage of someone walking from a CCTV system that will not be used in an automated biometric system
A recording of someone's voice which will be analysed by a biometric system to identify that person.	A recording of someone's voice that is not analysed by a biometric system e.g. a recording of a call taken for record-keeping purposes.
Information about someone's mood which you learn about through analysis by a biometric system.	Information about someone's mood which you learn about through the person taking a survey.
Numerical information extracted from an image of someone's face to represent their features (biometric template).	A DNA or blood sample.

Biometric processing

Biometric processing means comparing or analysing biometric information, using a **biometric system**.

Biometric processing includes:

- **Biometric verification**, which means comparing a person's biometric information against information previously provided by the person, to confirm the person's information matches. It asks the question "*Is this person who they say they are?*". Verification is often used as a security measure to protect personal information or prevent fraud e.g. when someone uses an electronic passport gate at the airport. Verification is sometimes called one-to-one (1:1) matching.
- **Biometric identification**, which means comparing a person's biometric information against information held in the biometric system, to identify the person. It asks the question "*Who is this person?*" or "*Do we know this person?*". For example, a body corporate could use a system to identify apartment owners and facilitate access to a building complex, or law enforcement might use it to identify persons of interest on a watchlist. Biometric identification is sometimes called one-to-many (1:N) matching.
- **Biometric categorisation**, which means analysing characteristics about a person to learn certain things about them, e.g. using a biometric system to detect someone's emotions, infer their gender from video footage or estimate their age from their face. More information about biometric categorisation is included further below.

A **biometric system** is a machine-based system that is used for biometric processing, e.g. computer software or an algorithm. It includes systems that involve some level of human input, assistance or oversight, but not systems that are solely or primarily dependent on human analysis.

Examples of biometric processing under the code	Not biometric processing under the code
Using a machine-based facial recognition system to identify when individuals in a database enter your business, and a staff member confirms how to respond.	Having a staff member with a list of people's faces look out for those individuals.
Using a software program to automatically compare someone's driver's licence against another photo of that person to confirm that it is the same person.	Manual comparison of a driver's licence with another photo to confirm the person is the same.
Using an algorithm to produce a list of possible identities of a person based on their face.	Having a staff member manually produce a list of possible identities of a person.
Automated analysis of CCTV footage to identify when an individual is at a site.	Manual review of the CCTV footage.
Use of age-estimation software to estimate age of users based on facial features	A staff member conducting a manual assessment of customer age demographics.

Note: The Information Privacy Principles (IPPs) apply to personal information that is not covered by the Code.

More information about biometric categorisation

Biometric categorisation is when you use an automated process to analyse biometric information to collect, infer or detect certain types of sensitive information or to categorise the individual by a demographic category.

The types of sensitive information and the demographic categories that biometric categorisation cover are:

- Health information e.g. information about a person's health conditions.
- Information about a person's personality, emotions, or mental state e.g. if someone is extroverted or introverted, how they are feeling, if they intend to lie, or if they are distressed.
- Information about a person's fatigue or attention levels e.g. whether someone is tired or paying attention to a specific thing.
- Any demographic category assigned to an individual because of a characteristic such as their physical features or how they act e.g. age, gender or ethnicity. The demographic categories covered by biometric categorisation include any demographic category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993.

Biometric categorisation does **not** include detecting a **readily apparent expression**, which is something you can observe or record visually or aurally without using biometric processing. For example, whether an individual is smiling or nodding, the level of their voice (whispering or shouting), or whether the individual uses a wheelchair or is wearing a mask.

Biometric categorisation also does **not** include any analytical process that is integrated in a commercial service, including any consumer device, for the purpose of providing the user with health information, personal information, entertainment or an immersive or lifestyle experience, provided that:

- The analytical process cannot be used separately from the commercial service, and
- The purpose or effect of the integration of the analytical process does not circumvent the rules in the Code.

This exception covers analytical processes in devices for consumer use like smartwatches, fitness trackers, or VR headsets. It also covers processes such as

filters that categorise body parts for a virtual clothing try-on service or editing software that categorises people in photos or videos to modify or sort them, provided in each case that the way the analytical process operates meets the definition above.

Some common types of biometric information

There are many different types of biometric systems and possible uses for biometric information. Some of the most common types of biometric information/biometric systems are:

- Face images (facial recognition technology or FRT).
- Eye scanning (scanning the iris, retina and/or sclera).
- Fingerprint and/or palm prints (can also include information about the surfaces of the hand itself).
- Gait (how someone walks, e.g. stride length and speed).
- Keystrokes (how someone types, e.g. the time taken on a sequence of keys, the rhythm of keystrokes).
- Voice (how someone sounds when they speak).

What doesn't the Code apply to?

The Code does not apply to health agencies or health information in some situations

The Code does not apply to biometric information if:

- that biometric information is also health information under the Health Information Privacy Code (HIPC), **and**
- the biometric processing is being done by a health agency.

In that case, the HIPC applies instead.

"Health agency" is defined in the HIPC. It includes any agency that provides health or disability support services, agencies which train health practitioners and agencies

which provide health, disability, accident or medical insurance (but only in respect of providing the insurance). For the full definitions of health agency and health information, see the HIPC.

If a health agency is doing biometric processing on biometric information that is **not** health information, the Code still applies. The Code also applies to biometric information that is also health information if the agency doing the biometric processing is **not** a health agency.

For example:

- A medical practice has fingerprint scanning to allow staff to enter the premises. This is not health information, so the Code applies.
- A medical practice uses biometric processing to help detect health conditions. This is health information, and the biometric processing is by a health agency, so the Code does **not** apply (but the HIPC would).
- A health and fitness club uses a biometric system to analyse the health status of its members. This is health information, but the biometric processing is not by a health agency (because the agency is not providing health services), so the Code applies.

Some rules in the Code do not apply to intelligence and security agencies

Rules 2, 3, 4(b) and 10(4) do not apply to the New Zealand Security Intelligence Service and the Government Communications Security Bureau. This mirrors similar exclusions in the Privacy Act and reflect the special nature of intelligence and security agencies' work.

The Code will generally not apply to consumer devices

As outlined above, in most cases devices for consumer use like smartwatches, fitness trackers, or VR headsets will not be covered by the Code. This is because these devices will not be doing biometric verification or identification, and if they are doing biometric categorisation, they would generally be excluded by the "integrated analytical feature" exception discussed in the biometric categorisation section.

In some cases, the way these devices work may mean that there is no organisation that is "collecting" information through the device, if the organisation has not taken any step to seek or obtain the information. This is a factual analysis that will depend on the specific situation.

The Code will generally not apply to individual people in their personal capacity

As with the Privacy Act, people acting in their private capacity would only be subject to the rules in the biometrics Code if what they are doing is either unlawful or considered "highly offensive to a reasonable person." (Section 27 of the Privacy Act)

If an employee is using biometric processing in their workplace, then the organisation would be responsible for the activity being carried out in compliance with the Code.

If a person is using biometric processing for a business or non-personal use, on their own account (e.g. as a sole trader) then the person is responsible for compliance with the Code.

Overview of the Code

There are 13 rules in the Code. Each rule modifies or otherwise applies the corresponding Information Privacy Principle (IPP) from the Privacy Act. More detailed information on the rules, as well as examples of how the rules apply, is available from page 21 of the full guidance.

Rule 1 – Purpose of collection

Rule 1 says you must not collect biometric information unless:

- It is for a **lawful purpose** connected with your functions or activities,
- It is **necessary** for that purpose,
- The risks and impacts on individuals from the biometric processing are **proportionate** to the benefit to you, the individuals or the public from the processing, and
- You have adopted and implemented **privacy safeguards**.

Whether biometric processing is necessary for your lawful purpose depends on whether the processing is **effective** in achieving your lawful purpose, and whether you could reasonably achieve the same purpose by an **alternative** form of processing that has less privacy risk. The alternative could be non-biometric processing, or it could be a different kind of biometric processing.

In some cases, you may be able to run a trial to assess whether the biometric processing is effective.

When considering whether the biometric processing is proportionate, you need to consider the degree of privacy risk, the cultural impacts and effects of the biometric processing on Māori, and whether the overall benefit is sufficient to outweigh the privacy risk and any negative cultural impacts on Māori.

Privacy safeguards are any action or process you take to reduce the privacy risk. Some examples of safeguards are ensuring the biometric system has been sufficiently tested and your staff are appropriately trained, but you need to consider what is relevant and reasonably practicable in your circumstances.

Finally, rule 1 also says that you may not require identifying information if it is not required for your lawful purpose.

Rule 2 – Source of biometric information

You must collect biometric samples directly from the person whose biometric information it is.

There are some exceptions in rule 2 that allow you to collect biometric samples from other people, for example if it is necessary to maintain the law, or if collecting it directly from the person would be prejudicial to that person or to the purpose of collection.

Rule 3 – Collection of information from individual

Rule 3 is about what you have to tell people when you collect their biometric information. There are some things you need to tell people before or at the time you collect their biometric information, for example why you are collecting their

information (the minimum notification rule). This information needs to be communicated to people in a clear and conspicuous manner.

There are also other things you need to tell people before you collect their biometric information, or if that is not possible, as soon as possible after you collect their biometric information. For example, the name and address of the organisation that is collecting the information.

You do not need to tell people the information in rule 3 again if you have already told them the same information on a recent previous occasion. There are also exceptions that allow you not to tell people about the things that rule 3 requires, for example if it would prejudice the purpose of collection.

Rule 4 – Manner of collection of biometric information

You must only collect biometric information in a way that is lawful, fair and does not unreasonably intrude into the personal affairs of the person whose information you collect.

What is fair will depend on the overall circumstances, including whether you are collecting information from children or young persons.

Rule 5 – Storage and security of biometric information

If you hold biometric information, you need to ensure that you protect the biometric information using security safeguards that protect against loss and unauthorised access, use, modification or disclosure of that information. The security safeguards you use need to be reasonable in the circumstances, which means it may change depending on what information you hold and why.

If you need to give someone access to the information so that they can provide a service for you, you must do everything reasonably within your power to prevent unauthorised use or unauthorised disclosure of the information.

Rule 6 – Access to biometric information

Individuals are entitled to receive from an organisation, on request:

- confirmation of whether the organisation holds any biometric information about them; and

- confirmation of the type of biometric information the organisation holds about them; and
- access to their biometric information.

Rule 7 – Correction of biometric information

Individuals have the right to request that an organisation correct any biometric information it holds about that individual.

Organisations do not have to correct information in the way that an individual requests. But, individuals have the right to give a "statement of correction" to an organisation that states how the individual wants their information to be corrected. The organisation must then take steps to ensure the statement of correction is attached to the biometric information so that it is always read with the information, and it must also tell any other person that it has disclosed the information to about the statement of correction.

Rule 8 – Accuracy of biometric information

You must take reasonable steps to ensure that biometric information you use or disclose is accurate, up to date, complete, relevant and not misleading.

Rule 9 – Retention of biometric information

You must not keep biometric information for longer than is required for the purposes for which it may lawfully be used.

Rule 10 – Limits on use of information

Rule 10 is about what you can use biometric information for. You can only use biometric information for the purpose it was collected for, unless an exception applies e.g. if the new purpose is directly related to the original purpose, or if the new use is necessary to prevent a serious threat to health or safety.

Rule 10 also contains fair use limits. These are limits on what you can use biometric information and biometric processing to do. You must **not** use biometric processing to collect, obtain, create, infer or detect (or attempt to collect, obtain etc):

- health information

- personal information about a person's personality, mood, emotion, intention, or mental state (except for information about a person's fatigue, alertness or attention level)
- information to categorise a person according to a demographic category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993 (except for the age of the individual).

However, there are exceptions to the fair use limits. For example, you may use biometric processing to collect information that would otherwise be restricted, if it is necessary to assist the person with accessibility or lessen a serious threat to public health.

Finally, rule 10 has a similar assessment to rule 1, (but applying to the **use** of information, not the collection) that says you must not start using biometric processing on personal information you already hold, or use information in a different kind of biometric processing

unless:

- it is necessary for your lawful purpose,
- the risks and impacts are proportionate to the benefit, and
- you have implemented appropriate privacy safeguards.

As with rule 1, whether your use of biometric information is necessary depends on whether it is effective in achieving your lawful purpose and whether your lawful purpose could be achieved by an alternative with less privacy risk. This restriction in rule 10 is to avoid a loophole where organisations could start using biometric processing on information they already hold.

Rule 11 – Disclosure of biometric information

You must not disclose biometric information that you hold to another person or to any other organisation unless you have reasonable grounds to believe that one of the exceptions in rule 11 applies. Some exceptions are:

- The disclosure of the biometric information is one of the purposes for which it was collected.
- The disclosure is authorised by the person whose biometric information it is.
- The disclosure is necessary to maintain the law or to lessen a serious threat to life or health.

Rule 11 is also subject to rule 12.

Rule 12 – Disclosure of biometric information outside New Zealand

You must not disclose biometric information to anyone outside New Zealand unless you have reasonable grounds to believe that one of the exceptions in rule 12 applies. Some exceptions are:

- The disclosure is authorised by the person whose biometric information it is, after being expressly informed that it may not be protected overseas in the same way as it is in New Zealand.
- The overseas person or organisation is subject to privacy laws that overall, provide a comparable level of protection as the Code.
- The overseas person or organisation is otherwise required to protect the information (for example, through a contract) in a way that overall, provides a comparable level of protection as the Code.

Rule 13 – Unique identifiers

You may only assign a unique identifier that is a biometric feature or a biometric template to an individual for use in your operations if that identifier is necessary to enable you to carry out your functions efficiently.

You also may not assign a unique identifier to someone that you know is the same as the unique identifier that another agency has assigned to the same individual.

“Assigning” a unique identifier means that the identifier is used as the means of uniquely identifying an individual in the organisation’s systems to be able to bring up information the organisation holds about that person.

There are some other technical restrictions on the use of unique identifiers. See our IPP 13 guidance for more information.

General good practice guidance on biometric processing

Privacy Impact Assessments

A key way for organisations to assess and address privacy risks when collecting, using or sharing biometric information is to do a Privacy Impact Assessment (PIA). We have guidance to help organisations do PIAs well.

Doing a PIA will help you check whether your planned biometric processing complies with the Code and help identify and minimise privacy risks. You don't have to use our PIA template, but all organisations should be doing sufficient planning and privacy analysis before starting any biometric processing. Otherwise, you may not be able to comply with the rules in the Code.

Consulting with people about biometric processing

It is good practice to consult with people about your intended biometric processing, especially if you are planning something that is complex, high risk or involves vulnerable individuals. In some cases, you may also have an obligation under another law (e.g. employment law) to consult with people who may be impacted by your biometric processing.

If you are planning a consultation, it's important to consult with the right people. You should consider:

- Whose biometric information will be impacted? Can you consult with people on an individual basis? What about representative groups?
- Is it appropriate to consult with people who have technical, legal or cultural expertise in the area of your biometric processing?
- How will you let people know about the consultation? Are you allowing enough time for people to respond? Are you genuinely open to feedback and/or making changes?

- Have you considered specific consultation with Māori if that is necessary or appropriate for your project?

Complaints under the Code

The Code does not change the complaints process set out in the Privacy Act. We have guidance on responding to requests and complaints well that will also apply to complaints related to the Code.

It's important to know:

- Individuals can make a complaint if they feel their privacy has been interfered with because of an organisation's collection, use or disclosure of their biometric information.
- Individuals must make reasonable efforts to resolve their complaint directly with the relevant organisation. If the organisation provides a process for individuals to raise a concern or complain about their handling of their biometric information, and the individual makes reasonable efforts to resolve the complaint with the organisation following that process, OPC will generally take that as sufficient to then investigate the complaint.
- A failure to comply with any of the rules in the Code could cause interference with an individual's privacy. Individuals have the right to complain to OPC about any action that the Code applies to.