Biometric Processing Privacy Code - guide

Contents

Introduction to the guidance

This guidance on the Biometric Processing Privacy Code (the Code) is to help organisations and individuals understand the Code and how it applies to them. It explains how the Office of the Privacy Commissioner (OPC, we) expect organisations to comply with the obligations in the Code. OPC will use the guidance as a benchmark if we are investigating any complaints or compliance issues under the Code.

The Code contains the legally enforceable rules that organisations must comply with and takes precedence over the guidance.

Who does the Code apply to?

The Code applies to all organisations - businesses, government agencies, NGOs - that collect biometric information for biometric processing (with limitations). “Agency” is the term used in the Privacy Act, but we’ve used the term “organisation” in this guidance. Agency is defined in section 4 of the Privacy Act.

What does the Code apply to?

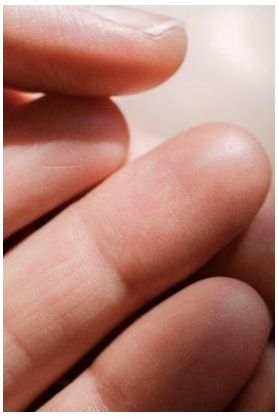
The Code applies to **biometric information** as a class of information and to the activity of **biometric processing** by a **biometric system**.

Biometric information

Biometric information is information about a biometric characteristic that is used for the purpose of biometric processing by a biometric system. Biometric characteristic includes:

- A person’s physical features e.g. their face, fingerprints, or iris.
- The way a person typically moves or acts with their body, e.g. the distinctive way a person walks, writes or types.

- A combination of physical features and how a person typically moves parts of their body, e.g. how a person sounds when they speak (the way a person sounds is due to both the shape of the vocal cords and throat and the distinctive way they use these structures to speak, producing accent, intonation, rhythm and speaking speed).



Biometric information also includes:

- A **biometric sample**, which is a record (either non-digital or digital) of an individual's biometric characteristic e.g. a physical or digital photo of a face, a scan of a fingerprint or a video of someone's gait when they walk. (These records are biometric information if they are used, or intended to be used, for biometric processing by a biometric system).
- A **biometric template**, which is a representation of information extracted from a biometric sample e.g. how an algorithm recognises and analyses the information in a biometric sample.

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.

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 (e.g. as used in facial recognition technology (FRT) or age estimation).
- Eye scans (scanning the iris, retina and/or sclera).
- Fingerprint and/or palm print scans (can also include information about the surfaces of the hand itself).

- Gait analysis (how someone walks, e.g. stride length and speed).
- Keystroke log (how someone types, e.g. the time taken on a sequence of keys, the rhythm of keystrokes).
- Pattern of device use / touch screen interaction (the way you use a smartphone e.g. the distinctive position, pressure and speed of someone's fingers when they swipe, scroll or tap)
- Voice audio (how someone sounds when they speak).

Biometric system

A biometric system means a computer- or technological-based system that is used for biometric processing. It includes any related devices and components needed to carry out the processing, such as cameras, scanners, comparison algorithm and tokens e.g. the FRT system used for border control uses ePassports (token) and eGates (camera and comparison process).

A biometric system typically uses both hardware and software elements to calculate an outcome (comparison score / match) or control a process (facilitate access) and may involve human input, assistance or oversight.

It does **not** include a system that relies **solely or primarily** on human analysis i.e. a purely manual system.

The key question is **who or what is analysing the biometric information**? If the analysis is being performed by the biometric system, then it will be included within the definition and subject to the Code. But if the analysis is solely or primarily done by a human, then it won't fall within the definition and won't be subject to the Code. If it is not subject to the Code, it will still be subject to the Privacy Act.

Examples of biometric information covered by the Code	Examples of information not covered by 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 processed in a 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**, to either verify, identify or categorise a person.

Biometric processing covers:

Biometric verification is the automated verification of an individual's claimed identity. It involves comparing a person's biometric information with other biometric information that has been previously associated with them (e.g. previously enrolled in the system or in an identity document) to confirm whether they match (i.e. are sufficiently similar). 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 is the automated recognition of a person's biometric characteristic (e.g. face, fingerprints etc) to identify them by comparing their biometric information against the biometric information of multiple people held in the system. It asks the question "*Is this person on the database?*" or "*Do we know this person?*". Identification is used to identify people who are allowed to enter a space and facilitate access to that space, 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 means analysing a person's biometric information 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.

Examples of biometric processing activities covered by the code	Examples of activities not covered by 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.

Examples of biometric processing activities covered by the code	Examples of activities not covered by the Code
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 using their human judgement to estimate customer's age.

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

Biometric categorisation

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

Biometric categorisation covers the collection or inference of the following types of sensitive information:

- **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, education level or ethnicity. This includes any demographic category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993.

Not biometric categorisation

Detection of readily apparent expressions

Biometric categorisation does **not** include using a biometric system to detect readily apparent expressions, gestures or movements which are things you can observe or record visually or aurally without using biometric processing. For example, whether an individual is nodding or has their eyes closed, whether they are whispering or shouting, or whether the individual uses a wheelchair or is wearing a mask.

This exclusion means that, in general, processes that detect aspects of a person's face or body to apply a filter or virtual try-on feature, or editing software that categorises people in photos or videos to modify or sort them, will **not be subject to the Code** (but may still be subject to the Privacy Act).

Personal use and entertainment exclusion

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

In general, processes in consumer wearables (e.g. in fitness trackers) that provide the user with their information or processes in face and body tracking cameras used to facilitate immersive video games (e.g. in VR headsets) will **not be subject** to the Code (but may still be subject to the Privacy Act).

Biometric categorisation examples

See rule 10 for more information about the limits on biometric categorisation.

Biometric categorisation includes collecting, obtaining, inferring or detecting…	**For example, using an automated process to…**
Health information. (See also the section on when the Code applies to health agencies.)	• Infer BMI from fingerprint data. • Detect skin condition from facial image. • Infer genetic disorders by mapping facial features. • Infer mental health status from eye movements. • Infer neurodegenerative condition from way individual writes / handwriting. • Detect if individual has prosthetic from gait or arm movements. • Infer stress level from voice.
Personal information relating to an individual's **personality.**	• Detect level of agreeableness through analysis of facial expressions. • Infer individual's level of emotional stability from eye and hand movements when talking. • Analyse a person's speech patterns and gestures to infer whether they are extroverted. • Infer an individual's susceptibility or openness from voice (e.g. for telemarketing).
Personal information relating to an individual's **mood.**	• Analyse micro expressions to infer whether individual is calm or irritated. • Detect a person's change in mood from body movements. • Detect excitement by measuring heart rate (HR) and heart rate variability (HRV). • Infer depressed mood from body posture.

	• Infer from voice whether individual is satisfied.
Personal information relating to an individual's **emotion.**	• Detect surprise or shock by registering minute facial movements. • Detect shame from body posture. • Infer positive emotion from heart rate and heart rate variability. • Detect sadness or anger in a person's voice.
Personal information relating to an individual's **intention.**	• Analyse micro expressions to detect intention to take aggressive action. • Detect intention to lie by monitoring eye movements and pupil dilation. • Analyse gait to detect intention to avoid detection. • Analyse typing patterns or handwriting to detect intention to deceive. • Infer intention to steal based on body and head posture. • Analyse voice to infer intention to leave conversation. Note: **readily apparent expressions** are excluded from the biometric categorisation definition: e.g. inferring that the wearer of a VR headset wants to go in a certain direction from their gaze or movements that is externally observable without automated processing.
Personal information relating to an individual's **mental state.**	• Infer interest and engagement from micro expressions. • Infer cognitive load from pupil dilation.

	• Obtain information about a person's state of distress from voice.
Personal information relating to an individual's **state of fatigue.**	• Infer how well rested a person is from the appearance of their eyes and skin. • Track eye movements or blink rate to detect fatigue. • Infer exhaustion level from voice.
Personal information relating to an individual's **alertness.**	• Detect hyper-vigilance from facial expression and pupils. • Detect arousal intensity via galvanic skin response. • Detect whether someone is sleepwalking from eye and body movements.
Personal information relating to an individual's **attention level.**	• Analyse facial expression to determine if engaged. • Monitor eye movements (gaze, blink rate) to detect level of focus. • Infer from sound of voice whether distracted.
To categorise the individual as part of a **demographic category** assigned to an individual on the basis of a biometric characteristic	• Inferring sex or ethnicity from facial features. • Estimating age from face shape and features. • Inferring socioeconomic status from skin condition. • Estimating age from gait or signature. • Using step count and HR to categorise according to fitness level. • Detecting whether person is pregnant from gait. • Attempting to infer sexual orientation from voice pitch and tone. • Inferring education level from sound of voice.

Biometric categorisation does not include…	For example…
Detecting a **readily apparent expression.**	• Detecting whether someone has their eyes closed or is speaking. • Creating realistic avatars that reflect the facial movements of the user. • Photo editing software that allows adjustments or changes to a person's physical appearance. • Detecting position of eyes, nose and mouth to apply a filter or virtual try-ons. • Detecting hair colour from facial image • Posture detection systems e.g. in yoga studios. • Collection and display of raw body metrics when exercising e.g. steps, cadence, heart rate. • Gesture controlled interfaces that detect conscious hand gestures i.e. swiping, waving, pointing. • Foveated rendering i.e. producing better graphics in the video game based on where user is looking. • Eye based interaction e.g. selecting menu items with gaze. • Voice pitch adjustment.
Personal use and entertainment exclusion: Any analytical process that is integrated in a commercial service, including any consumer device, solely for the	• Analysis of user's facial expression to infer emotions and mood while playing video game to adjust intensity of immersive experience. (Provided there is no other use by video game developer). • Photo/video app uses facial landmark detection to apply fun filters (e.g. dog ears, makeup, aging effects). (This would fall within the "entertainment

purposes of providing individuals with: their health information, their personal information or an entertainment or immersive experience.	or immersive experience" limb and may also be excluded under the readily apparent expression exclusion). • Inferring information about a person's condition (e.g. fitness level, daily energy level, stress) from their movement and heartrate metrics to display on their fitness wearable. (Provided the information is only for the user and is not used or shared by the app developer). • Car system detecting fatigue level of driver by analysing their voice commands and advising user to take a rest. (Provided the information not used for anything else). • Meditation app detects facial expressions and breathing movements via camera to reflect calmness on-screen to the user. (This would fall into providing the user with their personal information).

Other activities not covered by the Code

In general, the following activities will **not** be regulated by the Code as they do not fall within the definition of biometric categorisation (or verification or identification). These activities may still involve the collection and use of personal information, in which case the organisation carrying them out must comply with the Privacy Act.

- Face or person detection (without unique identification or demographic categorisation) e.g. detection of people on railway tracks, monitoring queues, smart cameras used on autonomous cars.

- Lexical sentiment analysis (tools that analyse the content of human speech or text and determine whether it is positive, neutral or negative or assign tags according to theme or topics, provided the analysis is based on the words as opposed to how a person says the words (tone, pitch etc.)).

If you are doing the above types of activities, you should still consider the definitions of biometric verification, identification and categorisation to be confident that your specific use is not covered by the definition.

Who 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 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" or "readily apparent expression" exceptions discussed in the biometric categorisation section.

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.

What if the Code doesn't apply?

The Privacy Act applies to personal information that is not covered by the Code. For example, the Act applies to any completely manual uses of biometric information.

The Privacy Act also applies to the results of biometric processing.

OPC's guidance on the Privacy Act and working with sensitive information continues to be relevant and applies to sensitive information that the Code does not apply to.

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 in the detailed guidance for each rule.

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,
- You have adopted and implemented **privacy safeguards**, and
- The risks and impacts on people, including Māori, from the biometric processing are **proportionate** to the benefit to you, the individuals or the public from the processing.

How do I demonstrate that a biometric system is necessary?

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 as effectively 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 and whether there is a reasonable alternative.

What are privacy safeguards?

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.

How do I assess whether my biometric system is proportionate?

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.

Rule 2 – Source of biometric sample

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 the person authorises you to do so, 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 (notification)

Rule 3 is about what you must 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 and if there's a non-biometric option (the **minimum notification rule**). This information needs to be communicated to people in a clear and obvious 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 in some cases allow you not to notify people. 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 and steps you take to obtain the information, including whether you are collecting information from children or young persons, what people's reasonable expectations would be in the context, and whether you are upfront or mislead people.

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.

This rule also means you need to make sure only that the appropriate people within your organisation are able to access the biometric information. This guards against employee browsing and misuse.

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.

Organisations are required to give reasonable assistance to people who wish to make or are making a request for access to their biometric information. Part 4 of the Privacy Act outlines how organisations should respond to access requests and situations where an organisation may withhold 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. This includes the right to request deletion.

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. You must delete or dispose of biometric information that you no longer need.

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. For example, 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 has limits on using information an organisation holds for biometric processing (if the information was not collected in accordance with rule 1).

Rule 10 also contains limits on **biometric categorisation**. These limits restrict using biometric information to categorise someone or infer sensitive traits unless an exception applies. For example, 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.

There are exceptions to the limits on biometric categorisation. For example, if it is necessary to assist the person with accessibility or lessen a serious threat to public health.

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 to avoid prejudice to the maintenance of the law or to lessen a serious threat to life or health.

Rule 12 – Disclosure of biometric information outside New Zealand

You must not disclose biometric information to anyone outside New Zealand unless you have a valid ground to disclose under rule 11 **and** 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 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.

General good practice guidance on biometric processing

Privacy Impact Assessments

The best 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 or cultural experts 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 people to raise a concern or complain about their handling of their biometric information,

and someone makes reasonable efforts to resolve the complaint with the organisation following that process (and has evidence e.g. correspondence with the agency), this is generally sufficient to show reasonable efforts.

- 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.

OPC's enforcement of the Code

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

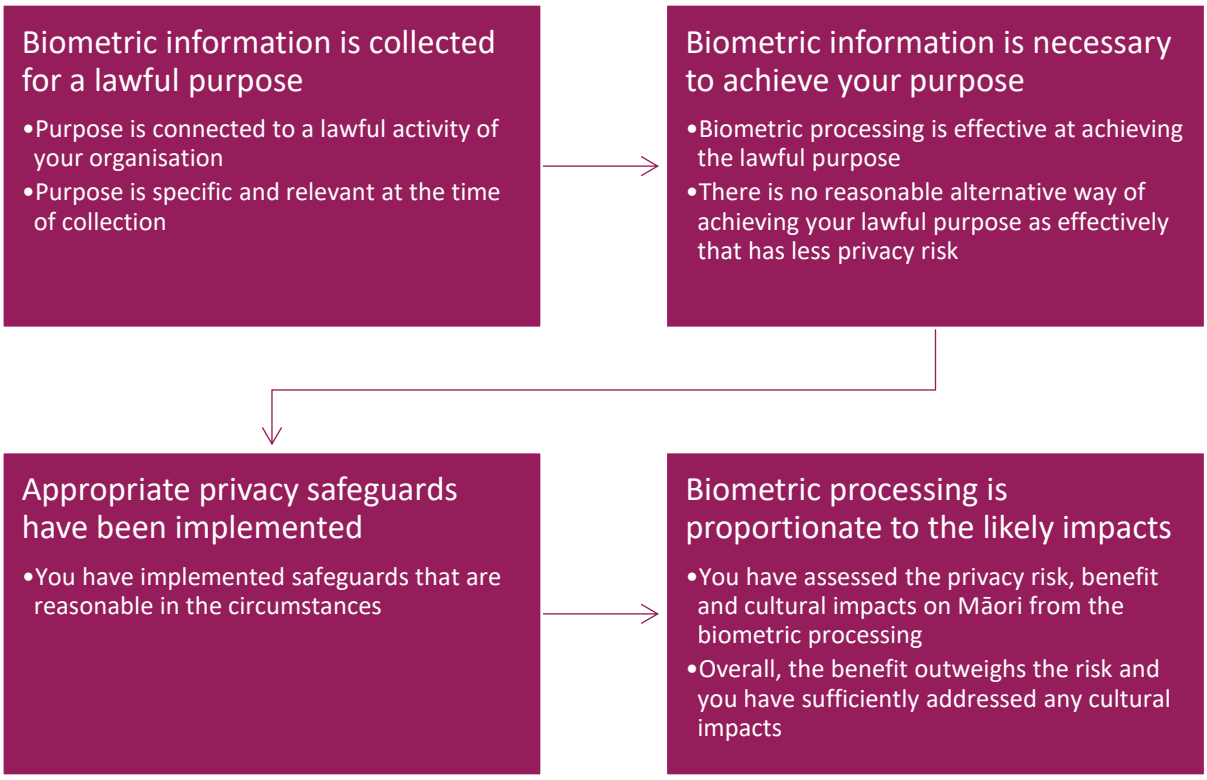
We decide whether and how to act based on several factors including the public interest, the seriousness of the potential breaches, the risk of harm of people and the conduct of the organisation.

Guidance on specific rules in the Code

Rule 1: Purpose of collection

Rule 1 is about your reason for collecting biometric information to use in a biometric system. You need to ensure:

1. Your collection of biometric information is for a **lawful purpose**.
2. Your collection is **necessary**, meaning it is an effective way of achieving your purpose and you cannot reasonably achieve your purpose as effectively by an alternative with less privacy risk.
3. You have implemented appropriate privacy **safeguards**.
4. Your biometric processing is **proportionate** to the likely impacts on people.



1. Lawful purpose

You need to identify a clear purpose that explains why you are collecting biometric information. Identifying a clear purpose will ensure you can properly walk through the rest of the rule 1 assessment: whether the collection is necessary and proportionate, what privacy safeguards are reasonable, and what the privacy risk is. It will also help ensure you can comply with the other rules in the Code.

Your purpose needs to be lawful – meaning it must comply with all laws, not just the Code or the Privacy Act.

Your purpose for collecting information should be specific – a purpose like “for business use” or “for security” is too broad. But the purpose can allow for multiple related uses –

provided that the purpose is still specific enough to allow people to clearly understand what the information is actually being collected for.

Your purpose for collection needs to be relevant at the time you are collecting information. You cannot collect biometric information just in case you may want to use it later.

The purpose needs to be connected to a function or activity of your organisation.

If your lawful purpose does not require the collection of a person's identifying information, you must not require that identifying information.

What if you delete the biometric information quickly?

"Collect" means to take any step to seek or obtain the information. Even if you delete the information quickly, you are collecting the information if you hold the information even for only a fraction of a second. But deleting the information quickly can be an important safeguard that helps you comply with the Code.

2. Necessary

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

For the biometric processing to be necessary, you need to be able to demonstrate that the collection of the specific biometric information is needed to fulfil your lawful purpose and that the information is relevant and not excessive or arbitrary. This requires that the collection is both:

- effective in achieving your purpose, and
- there isn't a reasonable alternative means that could achieve your purpose as effectively with less privacy risk.

The fact that biometric processing is available, convenient or desirable for you to use is not, on its own, enough to show that the collection of biometric information is necessary

for your lawful purpose. If you can achieve your purpose easily or effectively without biometric processing, it will be hard to show that it is necessary.

How much information you are collecting is relevant to necessity. The more information you intend to collect, the more difficult it could be to demonstrate that collecting **all** the information is necessary for your lawful purpose.

Effective

To meet the effectiveness requirement in the Code, there needs to be a clear and logical connection between collecting the specific information and fulfilling your lawful purpose. Effectiveness requires that the collection of the biometric information has a causal link with the achievement of your purpose. If the biometric processing does not directly enable the achievement of your purpose, then it is not necessary.

Effectiveness is about whether and to what extent the biometric processing achieves your specific purpose, not just about whether the biometric system can do what it is designed to do.

To test the effectiveness of a proposed use of biometric processing, you need a clear statement of the outcome you are seeking to achieve. What is the extent, scope and degree of the problem or opportunity you are seeking to address? You also need a detailed factual description of the measure you are proposing to implement and its purpose. The extent to which the measure you have proposed achieves this objective is how effective is it.

Assess the degree of effectiveness

The biometric processing needs to meaningfully contribute to the achievement of your lawful purpose for it to meet the effectiveness requirement in the Code. But how much it contributes to achieving your lawful purpose (i.e. the degree of effectiveness) is relevant both to whether your purpose can be reasonably achieved as effectively by an **alternative** means with less privacy risk and to the **benefit** of your processing, which forms part of the proportionality assessment.

Effectiveness is an ongoing requirement. You need to ensure that your processing remains effective once the system is in place. That means that you should continue to assess the kinds of evidence outlined below at reasonable intervals to ensure that your biometric processing is still effective. For example, you should reassess effectiveness whenever you make any substantial and material changes to the way your system operates.

What kind of evidence can show effectiveness?

There is a range of different types of evidence you can use to help assess whether the biometric processing will be effective. What is appropriate in your circumstances will depend on the overall risk and complexity of the biometric processing – high risk or complex uses of biometric information will require a more in-depth assessment. But, in every case you still need to have an objective basis for showing how the biometric processing will be effective in achieving your lawful purpose. More information on what makes biometric processing higher or lower risk is included in the privacy risk section.

Some examples of the types of evidence which can form part of your assessment of effectiveness:

- Performance metrics (e.g. accuracy metrics) from vendor or independent third-party.
- Information about training or evaluation data, including assessing differences between training data and likely real-world user data.
- Assessing the appropriate sensitivity and specificity setting for the use case.
- Evidence about the scientific or technical validity of the overall process to address the issue/problem.
- Running tests or simulations on training data in your particular context.
- Reviewing comparable uses or case studies from New Zealand or overseas (after identifying and adjusting for any material differences).

- Empirical evidence of effectiveness collected during a trial (see also the guidance below on trial periods). This could be evidence from your trial, or evidence from a trial by another organisation if the trial was in sufficiently comparable circumstances.
- Operational audits.
- Expert opinion(s) and academic or scientific research.
- Customer surveys to gain understanding of customer desire for improvements in experience/efficiency/convenience etc.

No reasonable and effective alternative with less privacy risk

If you can reasonably achieve your purpose as effectively through an alternative means with less privacy risk, then your biometric processing is **not necessary**. More information on assessing privacy risk is included in the privacy risk section.

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 your 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. A different biometric alternative could be using a verification system instead of an identification system, or collecting only one form of biometric information instead of multiple. The alternative option can also be a range of measures that you could reasonably implement – for example, using a combination of CCTV and security guards as an alternative to facial recognition.

The alternative **does not need to achieve the exact same outcome** as the biometric processing for it to be a reasonable alternative. The test requires an overall assessment of whether an alternative (or alternatives) with less privacy risk would be able to reasonably achieve your purpose as effectively. If so, the biometric processing is not necessary. But, if there is no reasonable alternative that would be able to achieve your

purpose as effectively, that can help you show that your biometric processing is necessary.

For example, in theory, a reasonable alternative to biometric-based ID verification could be manual ID verification. However, depending on your context, resources and other factors, the manual ID verification may not achieve the purpose as effectively as automated biometric-based ID verification would. For example, manual ID verification would not be as effective in a context where you need a high volume of highly accurate verifications that a client or customer can carry out remotely.

Running a trial to assess effectiveness and reasonable alternatives

The Code allows you to run a trial to assess whether your biometric processing will be effective in achieving your purpose, and whether your lawful purpose can reasonably be achieved as effectively by an alternative means with less privacy risk. If you opt to run a trial, you are able to defer compliance with the requirement to show that your processing is necessary (rule 1(b)) until the end of the trial when you will have more information about useful the biometric system is. You still need to meet all the other requirements of rule 1 and the rest of the Code.

See the guidance on running a trial for more information about when you can run a trial and what you should do before, during and after the trial.

> Note: A trial is different from testing your biometric system. A trial is used to evaluate real-world effectiveness. A test is a practice procedure carried out in a controlled environment to identify specific issues or assess if the system behaves as anticipated (without taking real-world actions).

3. Privacy safeguards

Rule 1 requires you to put in place reasonable privacy safeguards before collecting information. If a privacy safeguard is reasonable in the circumstances for you to adopt and implement, then you must do so before you start collecting biometric information.

What are privacy safeguards?

Privacy safeguards are measures that reduce privacy risk, increase the transparency and accountability of the biometric system, and increase the control individuals have over their information.

There are some examples of privacy safeguards below, but the list is not exhaustive. You can and should implement privacy safeguards that are not listed if they are relevant to your use of biometrics. You should also continue to assess safeguards throughout your use of biometrics to ensure your safeguards remain effective and appropriate – for example through regular audits, or whenever you make a material change to how your system works.

How do I decide which safeguards are "reasonable" to implement?

You need to consider the overall context and privacy risk of your biometric processing. Consider the kind of biometric system you will use, the relationship you have with affected individuals, the consequences if biometric information is lost, misused, inappropriately accessed or disclosed etc, and the likelihood of and consequences from errors in the biometric system.

A safeguard can still be reasonable in the circumstances to implement even if it is difficult, expensive or takes time to implement. You need to factor in the costs of relevant safeguards to your overall planning. But, a wholly disproportionate cost or difficulty to implement could make a safeguard no longer reasonable.

The more severe the consequences for individuals from misuse of their biometric information, or errors in the biometric system, then the more likely it is that a safeguard will be appropriate, even at a high cost or difficulty to implement.

Rule 1 requires you to ensure that the relevant safeguards are adopted or implemented before you collect information. You should continue to assess your safeguards for as long as you are collecting biometric information and make any changes that are necessary to ensure your safeguards are appropriate and effective.

Examples of specific safeguards

Authorisation and/or providing an alternative

Giving individuals the choice to authorise the biometric processing or use an alternative to biometric processing is an important safeguard to mitigate privacy risk because you give them control and agency over the collection of their personal information. It won't always be appropriate – for example, in some contexts like fraud prevention, requiring or even offering authorisation may undermine your lawful purpose. However, if it will not undermine your lawful purpose, organisations should consider whether individual authorisation and/or providing an alternative is reasonable in the circumstances, particularly if you have a direct interaction with the individual you are collecting information from.

If you are implementing individual authorisation as a safeguard, you should consider:

- Has the individual been specifically and meaningfully informed about all the relevant factors involved in the biometric processing – e.g. what information is being collected, why, who has access, how it will be stored and used, and how it will be protected?
- Is there a genuine non-biometric alternative available? It should be a genuine choice for the individual as to whether to authorise the processing or whether to use the alternative. This does not mean that that individual gets to choose the consequences of not authorising the processing – but the option to authorise should not be coerced or presented in a way that leaves the individual with no effective choice. Remember that if you can reasonably achieve your lawful purpose as effectively by an alternative means with less privacy risk, then your biometric processing will not be necessary. But there may still be less effective non-biometric alternatives that are reasonable to offer individuals as an alternative.
- Is there an easily accessible way for the individual to withdraw their authorisation at any point without being penalised?

- Is there is an imbalance in power between you and the individuals who are being asked to authorise the biometric processing? For example, employers, public agencies or any agency where people may depend on the services provided by that agency for basic needs? If so, you need to take special care when relying on authorisation. People may have no other viable option, and could be worried about negative consequences if they do not authorise the biometric processing, which may make the authorisation not freely given.

You should not make unnecessary obstacles that would prevent individuals choosing the alternative to biometric processing, such as by requiring additional information, unnecessarily delaying access to services, hiding or de-prioritising the alternative option, or penalising the individual for choosing an alternative. You should also consider accessibility for people with disabilities to ensure your alternative does not exclude anyone.

If you are using authorisation as a safeguard, then the authorisation must be explicit. You cannot rely on assumed or implied authorisation – for example, continuing to use a service, or entering a space where biometric information is collected (e.g. a store using a FRT system) would not be sufficient evidence of authorisation. You should also seek fresh authorisation for any material changes in how you collect, use, hold or disclose information.

Example:

A fitness gym plans to use FRT for members to access its facilities. Individual authorisation and a non-biometric alternative could be used as a useful safeguard to reduce privacy risk by having a specific entry gate where the FRT would not operate, and individuals could instead use a swipe card.

However, if members were told that if they do not authorise the biometric processing, they can no longer access the gym but still have to pay membership fees for the rest of their contract, then this would not be reasonable implementation of authorisation as a safeguard because the individuals were not given a genuine choice.

Safeguards for biometric watchlists

A watchlist is where you have a list of specific individuals whose information is enrolled in your biometric system and who you want to identify to take some kind of adverse action against them – for example, removing them from your premises, monitoring their behaviour or imposing a fine on them. If you are using a biometric system to operate a watchlist, there are some key safeguards you should implement to help mitigate the privacy risks.

It is not necessary for you to know the names or any other details of people on your watchlist.

First, when deciding whether to add someone to a watchlist, we expect:

- Adding each specific person must be clearly linked to achieving the lawful purpose of the biometric processing.
- Only collect information for the watchlist in a fair and reasonable way.
- There are objective and consistent enrolment criteria. This helps mitigates the risk of subjective decision making that could perpetuate unfairness, bias or discrimination.
- Manage decisions about enrolment with a small and well-trained group of people.
- Do not add children and young people or other vulnerable people to a watchlist unless there are special circumstances that justify their inclusion.
- You should generally only use objectively verifiable facts to make enrolment decisions (e.g. a conviction, clear evidence of relevant behaviour, or a trespass notice). If you add someone to a watchlist based on opinion or speculation, this has more risk – both for the person concerned and for the agency – than verified information.

The minimum accuracy match threshold should be carefully considered and appropriate to your circumstances.

In addition, if you are operating a biometric watchlist, in general you should **inform** an individual on the watchlist of the following matters, (unless doing so is not practical in the circumstances):

- When they are enrolled in the biometric system.
- How they may challenge their enrolment.
- If an adverse action is taken or is to be taken, and what the consequences of that action are.
- How the individual may challenge a decision to take an adverse action.

You should also delete any biometric information of individuals not on the watchlist as soon as it is determined that they are not a match to an individual on the watchlist. For example, if you are using a FRT system to identify specific individuals, you should immediately delete the biometric information of anyone not on the watchlist.

In some situations, informing individuals about their inclusion on the watchlist will not be appropriate or feasible, for example if you do not have the individual's contact details, if it is not safe to approach the individual or if informing the individual would undermine the purpose of the biometric watchlist. However, if you can't notify individuals directly, you should still consider whether you can provide general information about the watchlist e.g. on your website.

Examples:

- A store is using FRT to identify individuals on a watchlist. Individuals are enrolled on the watchlist if they are trespassed from the site because of violent or aggressive behaviour or high-value shoplifting. At the time that individuals are trespassed they are verbally informed that they are being enrolled in the store's watchlist and they are given a notice explaining the store's process and the consequences for the individual. Informing the person of these matters does not undermine the purpose of the watchlist, so it is reasonable to implement this

safeguard and inform people of their inclusion on the watchlist. Biometric information of people not on the watchlist is immediately deleted once it is determined the individual is not on the watchlist.

- FRT is being used at a train station to manage a watchlist of people who have made violent threats. Informing the people directly could endanger staff, so information about the existence of the watchlist is included on a website instead.

Testing and/or assurance of the biometric system

The biometric system should be subjected to testing and/or assurance processes before you collect any biometric information. This could involve:

- Reviewing any external evaluation of a biometric system's performance.
- Testing the biometric system with test data.
- Testing the impact of different matching thresholds to assess false positive and false negative rates.
- Establishing a process for dealing with false matches and false non-matches.
- Testing for and mitigating any identified bias in the system (for example, lower accuracy rates for certain demographic groups). If the bias could lead to discrimination, you should not use the system unless the bias can be sufficiently mitigated to a level that no longer carries a significant risk of discrimination.

You may be able to rely on the testing done by a provider of the biometric system – particularly if the overall risk of your use of biometrics is low. However, you still need to ensure you have sufficient confidence that the testing was sufficient for your purposes – for example, by seeking evidence of the testing and assessing whether you need to do additional independent testing. Additional testing or assurance may be particularly relevant if you are using FRT, given the lack of existing testing on New Zealand faces.

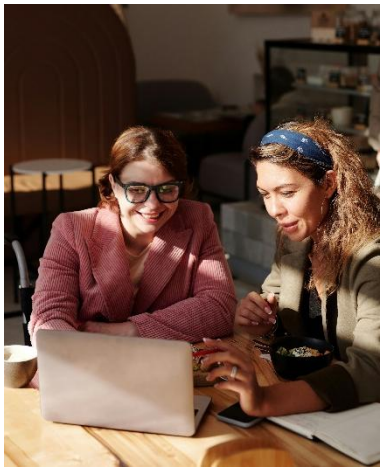
Your testing process should also help you identify what other safeguards are necessary to have in place to reduce the risk that individuals may suffer real detriment or harm because of errors or false matches or non-matches by the system.

Protect biometric information with security safeguards

You need to have a plan for how you are going to keep information secure before you collect it, including by considering any security issues with using a third-party provider.

Some security safeguards which will generally be relevant for organisations to implement are:

- Use multi-factor authentication to protect access to biometric information.
- Encrypt biometric data that you store.
- Process biometric samples into biometric templates as soon as possible and destroy the original sample.
- Use Privacy Enhancing Technologies (PETs). The Information Commissioner's Office in the UK has more guidance on using PETs.
- Store biometric information separately from other personal information you hold about an individual.
- If you are using a third-party provider of a biometric system, ensure your contract contains privacy-protective obligations on the provider. Also ensure you have reviewed the provider's own privacy policies and practices. See our guidance on working with third-party providers for more information.
- If it is necessary to give biometric information to a person or other agency in connection with the provision of a service to your organisation, ensure



that there are sufficient security safeguards in place to receive and access the information.

- Engage a subject matter expert to review your security controls.

OPC has further guidance on Security and Access controls in Poupou Matatapu, as well as our guidance on rule 5.

Human oversight and staff training

Having human oversight of your biometric system is an important safeguard. However, it is not enough to simply have human involvement – it is how people are involved that matters.

The human oversight or monitoring needs to be by individuals who have sufficient training to understand how the system works and what a match by the system means. They also need to have the confidence to overrule the system if there is a mistake. They need to be providing genuine scrutiny, not merely confirming results without proper assessment (e.g. due to "automation bias", which is the tendency for people to over-rely on automated systems when making human decisions).

Having effective oversight requires agencies to have process in place to:

- Provide sufficient training for people who will be establishing, overseeing and operating biometric systems, including regular refresher training.
- Support people to challenge results of the biometric system where necessary.
- Address issues of bias and discrimination. In some contexts, particularly for high-risk use cases with a high risk of harm to individuals, it will also be appropriate to consider training on internal/unconscious bias of the overseer that could be reinforced by the system.
- Make changes to the system to respond to errors or flaws.

- You should keep a record of all staff training. You should update your training any time there is a material change in the biometric system and any time you identify any issues with how the staff are monitoring the system.
- Staff should have general privacy training in addition to biometric-specific training.

Review and audit the biometric system

You should regularly review and audit any biometric system and the safeguards that are in place. This can be done by your organisation, but you should consider whether to use an external party to review and audit the system. Where the overall privacy risk is higher, it will be more appropriate to have external review and audit.

The review and audit could cover the overall performance of the system, security safeguards, staff training, any adverse actions taken, how information has been used and disclosed, performance of third-party vendors, compliance with policies, protocols and procedures etc.

We expect organisations to continue to review and audit throughout the whole life of a biometric system. It will often be appropriate to conduct the reviews and audits at a higher frequency when the system is first being used, and again following any significant changes.

Maintain appropriate policies and procedures

You should have appropriate policies and procedures that govern the use of any biometric system. But it is not enough just to have the policies and procedures in place – they must be fit for purpose and followed by staff. These documents should be regularly reviewed and updated as necessary.

Policies and procedures should address:

- Overall compliance with the Code and the Privacy Act.
- Thresholds for matches and the process for reporting and addressing errors with the system.

- Training obligations.
- If operating a biometric watchlist, the process for adding or removing people from the watchlist and taking adverse action.
- Review and audit of the system, including user access.
- Governance of the system.

4. Proportionality

You must not collect biometric information unless you believe, on reasonable grounds, that the biometric processing is **proportionate** to the likely impacts on individuals. To assess whether the biometric processing is proportionate, you need to assess:

- The scope, extent and degree of **privacy risk** from your 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.

Privacy risk

A key part of the proportionality assessment is determining the degree of privacy risk presented by your use of biometrics.

Under the Code, privacy risk is any **reasonable likelihood** that the **privacy** of individuals may be **infringed** by the biometric processing. A privacy infringement is any impact or effect of the biometric system that may limit, undermine or encroach on an individual's privacy or deter individuals from exercising their rights.

The concept of infringement is broader than an interference with privacy (see section 69 of the Privacy Act) in order to take account of the subtler systemic or aggregate impacts of using biometric systems that erode people's privacy, like the impacts of monitoring public spaces, as well as distinct harms to individuals.

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

The Code lists examples of possible privacy infringements that can result from using a biometric system / biometric processing, which includes:

- You collect more biometric information or keep it for longer than is necessary.
- The biometric information collected is not accurate.
- There are security vulnerabilities affecting the information.
- There is a lack of transparency about how you are collecting biometric information.
- Individuals are misidentified or misclassified because of the biometric processing, including where the misidentification or misclassification is due to differences in demographics such as race, age, gender or disability.
- An individual may have adverse actions taken against them (e.g. a person is denied access to a service) or they may be deterred from exercising their rights (e.g. right to freedom of movement or freedom of expression) because of the use of biometric processing for the purposes of surveillance, monitoring or profiling. This risk could apply whether the surveillance, monitoring or profiling is done by a public or private organisation.
- There is an unjustified expansion of the use or disclosure of biometric information after it is collected.
- The ability of individuals to avoid monitoring is diminished in spaces where they may reasonably expect not to be monitored. Again, this risk is relevant regardless of whether the monitoring is done by a public or private organisation, and regardless of whether the monitoring occurs in a public or private space. “Monitoring” is more than just being seen or watched. Monitoring could include

that a person's actions or movements are specifically followed, noted, or a decision is made because of what the person does.

- Any other infringement of the privacy interests of individuals or any other infringement of the protections for biometric information in the Code.

Although the Code lists certain privacy risks that you must consider, the context of your biometric processing is key to understanding the privacy risk, and you may need to take into account risks that aren't listed in the Code.

Note: requiring that agencies take into account the risk of privacy infringements in the proportionality assessment does not change the threshold for a successful privacy complaint under the Code i.e. finding an agency has interfered with an individual's privacy through their use of a biometric system.

How to assess privacy risk

All biometric processing has some risk, but some forms of biometric processing are higher risk than others.

To assess the privacy risk posed by your biometric processing, you could use the following framework based around **what** information you are collecting, **whose** information it is, **why** you are collecting it, and **when**, **where and how** you are collecting it.

What – the volume and nature of the information

- What information are you collecting? How sensitive is that information? *(Information that is more inherently connected to a person, or is particularly revealing, difficult to change or hide will generally make information more sensitive).*
- How much information are you collecting? How many people's information?
- Could the information be used to reveal other information about a person or profile them?

- Can the information be easily linked with other information?

Who – who is the information about and who collects it

- Whose information are you collecting? Are they vulnerable in some way? Are they more likely to be negatively impacted by any bias or discrimination? e.g. children, minority group, experiencing distress or reduced capacity to exercise privacy rights.
- Is there a power imbalance between you and the people whose information you are collecting? e.g. – employer/employee, landlord/tenant, government agency with enforcement powers, a provider of critical service with few alternatives vs. a provider of non-critical service with lots of alternatives.
- Have individuals freely authorised the collection? Are there realistic alternative options if individuals want to opt out of biometric processing? *(Authorisation with a genuine alternative is an important risk mitigation if it is practical for your circumstances).*
- Have you consulted with people whose information will be collected?

Why – why are you collecting the biometric information?

- What is your purpose for collecting information? Is it broad and conceptual or clear and targeted? *(Impacts the risk of scope creep).*
- How complex is the use case? Does it involve multiple steps, dependencies, opaque systems, information flows or discretion? Or is it simple and straightforward? *(Impacts opportunities for misuse or failure, harder to maintain transparency and accountability).*
- What are the consequences, if any, for individuals? Is the system to support taking adverse actions against individuals? What would be the impact of errors or

inaccuracy of the system on individuals? Is there a contingency or backstop process? *(Impacts the likelihood and severity of harm).*

How – context and design of the system (including where and when it is operating)

For this dimension, think through the personal information lifecycle and your operational choices.

- How is the information collected? Covertly, remotely or directly? Actively or passively? (*Affects transparency and ability for individuals to exercise choice and privacy rights)*
- What is the context – public space, private space, retail, entertainment? Might the system deter people from exercising their protected rights or reduce the ability of individuals to avoid monitoring where they may not expect to be monitored? (*Public spaces, semi-public spaces or private spaces that are essential for individuals to access increases the risk because of the potential chilling effect and surveillance risks. Whereas non-essential private spaces, especially where individuals have a range of alternatives, will generally lower the risk*).
- How is the information processed? Live or retrospective? High- or low-quality inputs? Centralised or local processing? *(Relevant to surveillance, accuracy and data breach risks).*
- Is information stored? How long for? *(Likelihood of security risks).*
- How is the information protected? Who has access to information? What are the security controls? *(Likelihood of misuse, unauthorised access, information lost or stolen).*
- Is the information routinely or occasionally shared? Or collected, processed or stored on your organisation's behalf? What protections are in place? *(Risk of data breaches, unauthorised sharing or unlawful secondary use).*

- Are there policies around who can access the data and what it can be used for? Audit logs? *(risk of misuse, security breaches, unauthorised access)*

Some privacy risks in biometric systems are inherent and can't be changed. For example, why the information is collected (collecting for public surveillance will pose more risk than for 1:1 verification) or who the data is about (children or other vulnerable groups raises the inherent risk). Other risks can be managed or mitigated through design choices, including how much information much information you collect, how you collect, store and protect it, or how long you retain it.

Remember that privacy risks also arise in the collection and use of non-biometric information. Assessing the relative risk of biometric processing compared to processing of other personal information can form part of your assessment of whether there is a reasonably effective alternative with less privacy risk. See the section on alternatives for more detail.

Summary of lower and higher risk factors

This table provides a high level summary of factors that OPC may consider to increase or lower the privacy risk. Each assessment still turns on its own facts and you need to consider how your own context and specific processing impacts the degree of risk.

Factors that tend to lower risk	Factors that tend to increase risk
System's **scope** is limited or targeted **scope** of system, i.e. 1:1 verification, use impacts a small number of individuals or a select group.	System's **scope** is wide or indiscriminate, i.e. 1:N identification, use impacts many individuals or society more generally.

Factors that tend to lower risk	Factors that tend to increase risk
Likelihood of errors lower: • **High quality** biometric probes/references. • **Operation in controlled environment**	**Likelihood of errors higher:** • **Low quality** biometric probes/references. • **Operation 'in the wild'**
Established uses of biometrics with robust scientific basis and high accuracy.	**Emerging or novel uses** of biometrics with uncertain effectiveness and limited research/scientific basis.
Use in places where individuals would reasonably expect to be asked to confirm their identity.	**Use in public spaces**, or private/semi-private spaces where people don't expect to be monitored.
Minimal or no loss of autonomy or control. • **Individual authorises use** on a clear opt-in basis. • **Genuine alternative** easily available to them.	**Significant loss of autonomy or control** **No adequate notice.** • **Lack of authorisation**, unclear authorisation, or authorisation relied on without genuine alternative (if authorisation would be appropriate for the circumstances). • **No alternative.**

Factors that tend to lower risk	Factors that tend to increase risk
Little to no power imbalance between individuals and agency (e.g. a provider of an optional commercial service with lots of competitors, individual has high level of consumer power).	**Significant power imbalance** between individuals and agency (e.g. agency with law enforcement powers, a provider of a critical service with few or no competitors, employment relationship, meaningful/significant age difference).
Low impact on individual if a privacy risk eventuates e.g. system may inconvenience individuals or produce delays if it's inaccurate.	**High impact on individual** if a privacy risk eventuates e.g. causes inability to access a social or essential service, information or facility that individual is warranted to access, causes humiliation, distress or stress, or financial impact if system doesn't work properly.
Individuals who are the subject of processing **less vulnerable to privacy harms** e.g. have high capacity or ability to exercise privacy rights, not part of a vulnerable group in society, unlikely to experience bias.	Individuals who are the subject of processing more **vulnerable to privacy harms e.g. lower capacity or ability to exercise privacy rights,** individuals more likely to experience bias, part of a vulnerable group in society.
Examples: Verification to authenticate user or facilitate access.	Examples: Identification for surveillance, monitoring or profiling.

Look at the whole picture

Assessing the overall risk requires you to consider the biometric system as a whole and the context in which your biometric processing will take place. You need to consider all factors which increase or decrease your risk. The modifiable risk factors (such as what information is collected), are a way to mitigate the risk by changing how the system operates to reduce your overall risk. See the safeguards section for more ways that you can protect biometric information to lower the overall privacy risk.

Unacceptable risk

In some cases, there may be factors which make the risk unacceptable. For example, if you do not have sufficient security safeguards to meet the requirements in rule 5 to keep the information secure. Similarly, if the accuracy of the system is not high enough to meet the requirement in rule 8 to ensure information is accurate before use. If the risk is unacceptable, you cannot continue with collecting biometric information unless you can sufficiently decrease the risk.

Weighing benefits against risk

Adopting biometric systems should be driven by an analysis of the benefits and risks, rather than the availability or appeal of the technology. To support this, the proportionality assessment requires organisations to weigh up:

- the benefit of using biometric processing to achieve the lawful purpose

  against

- the scope, extent and degree of privacy risk.

This section discusses how to assess the benefit and how to do the weighing exercise; more guidance on risk is included in the privacy risk section.

Assessing the benefit of a biometric system

An organisation's purpose for implementing a biometric system is the reason the system is needed (the "why"). The benefit of a biometric system is the positive effect or value that results from its implementation (the "consequences from the why", or "why does the

why matter?"). The achievement of your purpose may also be your benefit if your purpose has been expressed in sufficiently specific terms.

Because a biometric system is an automated way of recognising someone or inferring certain traits, the benefits of using a biometric system will typically reflect the fact that it's an automated process. For example, increased efficiency, reliability or consistency, reduced manual errors (if the system is sufficiently accurate), faster turnaround times, quick decision making, user convenience and streamlining processes.

- **Example**: If an organisation wants to use a biometric system to verify clients' identities as part of the organisation's obligations to prevent money laundering (the purpose of collecting biometric information), the benefits of using the system might include: a high level of accurate verifications, increased convenience for most clients by allowing remote verification, reduction in time to process a verification, and removing the need to retain scanned copies of identity documents.

Be clear and specific

When assessing the benefit of achieving your purpose, you need to be clear on the specific benefit you expect to achieve and what kind of benefit it is (**public benefit**, benefit to the relevant **individual/s**, or private **benefit to the organisation**).

You should clearly document the benefit. Like your purpose, the benefit must be specific and directly linked to the biometric processing. For example, the benefit needs to be more specific than a generic "improved customer experience", or "improved safety" – be clear on the actual specific improvement and how it will be achieved through biometric processing. You should be able to explain what the problem is you are trying to solve, or what would happen without the biometric processing.

Examples of specific benefits:

- Benefit to the organisation: Increased security of access to a restricted information database by using fingerprint scanning as a form of multifactor

authentication. This will reduce the risk of unauthorised access to the restricted information.

- Clear benefit to individuals: Improved customer experience for entering facility through offering facial recognition as an alternative option to increase the speed of entry and eliminate the need to carry a physical access card, thus increasing customer satisfaction for those who choose to use the facial recognition option.
- Public benefit: Improved efficiency and security at the New Zealand border through the use of biometric-based passport controls.

The better the biometric system works, the greater your benefit

The benefit is related to how effective your biometric processing is in achieving the intended purpose – the more effective a biometric system is at doing what it was set up to do, the greater the benefits produced. The reverse is also true, less effective or unfit systems will provide fewer benefits, and it will be harder to determine that they are proportionate. (See also the section on effectiveness).

You also need to have reasonable grounds for assessing the scale of the benefit.

For example:

- What is the level of increase in staff and customer safety?
- To what extent can this increase be directly attributed to the biometric processing?
- What is the increase in the level of security of the information database?
- What is the expected improvement in customer satisfaction?
- How much more effective will the facial recognition system be over the existing process?

It is not necessary to have an exact percentage improvement, but you should have a general idea of how much benefit comes from the biometric processing– e.g. a

moderate improvement in customer safety or a small increase in security of information access.

Does the benefit of the biometric system outweigh the risk?

Once you have clearly established what the expected benefit of your biometric processing is, you need to consider whether that benefit outweighs the privacy risk, taking into account the different standards that apply to the categories of benefit. What you are asking is whether the benefit e.g. additional security, efficiency, time, convenience, user experience, reduced cost, justifies that risk that you identified when assessing your privacy risk.

As outlined above, a biometric system can benefit the public, the individual whose biometric information you are collecting, and/or the organisation collecting the biometric information. Depending on who is accruing the benefit of the system, the Code requires a slightly different assessment when considering whether the benefit outweighs the privacy risk:

- A public benefit needs to outweigh the privacy risk. A benefit is not a "public benefit" just because it may benefit some members of the public. A public benefit is when there is a benefit for a **meaningful** section of the public.
- A benefit to the individuals whose biometric information you're collecting needs to be a clear benefit, and it needs to outweigh the privacy risk. This means that the benefit to the individuals needs to be obvious and specific. For example, if the benefit to the individual is increased convenience, this should be an obvious and specific improvement for that individual – not just a general improvement in broader convenience that may or may not benefit that individual.
- A benefit to the organisation collecting the biometric information needs to outweigh the privacy risk by a substantial degree.

Public or customer opinion (e.g. that the public is supportive or not of the biometric processing) can be relevant to both the benefit and privacy risk but is not in itself

determinative. That is, just because a majority of your customers may support or not oppose the processing, does not mean that the benefit will outweigh the risk.

If your biometric system is high risk, you will need a correspondingly significant benefit for the processing to be overall proportionate. If your system is low risk, then it could be proportionate even if you have only identified minor advantages from using the system, like 50 percent more efficient and improved user experience. If your system presents a high level of risk, but you only achieve modest or limited benefits, you will need to modify the risk to be lower (see the guidance on privacy risk) or the processing will not be proportionate.

The rule 1 example scenarios show how the weighing exercise could work in practice.

What if my organisation is using biometric processing to achieve several different purposes and benefits?

If you intend to use biometric processing for multiple lawful purposes and the purposes have benefits in different categories, then you should consider the proportionality for each purpose separately, according to the relevant benefit for each purpose.

The purpose of your biometric processing needs to be proportionate when considering only one of the benefit categories. For example, if your purpose has advantages to multiple groups (e.g., there is both a public benefit and a clear benefit to the people subject to the processing), your system still needs to be proportionate based on just one of the benefit categories (i.e. you can't tally multiple small benefits to claim the system is proportionate).

Example: a retail store intends to use FRT for the purposes of improving staff and customer safety and preventing stock losses by generating alerts to guide an appropriate staff response when individuals on a watchlist enter the store. The store considers the proportionality of each purpose separately:

- There is a public benefit for the staff and customer safety purpose. To be proportionate this benefit needs to outweigh the privacy risk.

- There is a private benefit to the store from the loss prevention purpose. To be proportionate this benefit needs to outweigh the privacy risk to a substantial degree.

If you are running a trial, how do you meet the proportionality requirement?

If you are running a trial under rule 1 to assess how well the biometric system works, then you may not know in advance exactly how beneficial using biometrics in your context is, until after the trial is complete.

The Code requires that you have **reasonable grounds** to believe that your biometric processing is proportionate. This threshold (belief on reasonable grounds) is flexible depending on the circumstances. Therefore, if you are thinking about conducting doing a trial of a biometric system, you need to believe, with good reason, that the trial is a proportionate course of action given the privacy risks and likely or anticipated benefits).

We would expect there to be a reasonable and objective basis for your belief that at the end of the trial, there will be a benefit that outweighs the risk, assuming that the trial demonstrates that the system is sufficiently effective. See our trial guidance for more information on running trials.

Cultural impacts and effects on Māori

Part of determining whether your proposed use of biometrics is proportionate is working through the cultural impacts and effects of the biometric processing on Māori.

How would this affect your proportionality assessment?

The Code requires you to have reasonable grounds to believe that the biometric processing is proportionate to the likely risks and impacts on individuals, after specifically taking into account the cultural impacts and effects on Māori. Identifying and addressing cultural impacts and effects is a necessary part of the proportionality assessment.

Cultural impacts and effects could result from:

- Cultural perspectives (e.g. tikanga Māori, Māori data sovereignty, te Tiriti o Waitangi and He Whakaputanga o te Rangatiratanga o Nu Tireni) that affect how Māori view or are impacted by biometric processing.
- Any different impact the biometric processing has on Māori, for example discrimination against Māori due to bias in the biometric system (e.g. bias leads to adverse decisions against Māori individuals at a higher rate than non-Māori).

Māori perspectives on privacy and biometric information

Biometric information is of cultural significance to Māori

Personal characteristics such as a person's face or fingerprints are so inherent to the identity of a person that Māori treat them with special sensitivity. They are imbued with the tapu of that individual which restricts the way in which biometric information is engaged with. From a Māori perspective, tikanga (values and practices) such as tapu, whakapapa, mauri, noa, mana, hau and utu should influence how you collect, store, access, maintain and disclose biometric information.

Violations of biometric information require appropriate redress

A failure to observe Māori perspectives on privacy and biometric information may result in a hara or violation. In addition to any other harm, a hara creates a disparity between the parties involved. Such violations can impact the whakapapa, tapu, mana, mauri and hau of the affected party and must be corrected by the offending party, for example through an apology, karakia, reparation, rectification of the technology or finding alternatives for the individual to use.

Māori data sovereignty

Māori data sovereignty gives effect to the inherent sovereign rights and interests Māori have over the collection, ownership and application of their data as a taonga under te Tiriti o Waitangi. The principles of Māori data sovereignty are a self-determining framework that influences the way that Māori control their information, including biometric information. Te Mana Raraunga (the Māori Data Sovereignty Network) have

outlined how key principles translate to concrete ways to protect Māori data and can help all organisations consider how the use of biometrics could impact and affect Māori.

Government agencies must consider te Tiriti

Government agencies will need to consider any use of biometric information in the context of te Tiriti obligations and while considering the power imbalance between the Crown and Māori. For instance, how do principles such as tino rangatiratanga and partnership impact the use of Māori biometric information?

Definitions for key concepts

- **Mātauranga:** Māori knowledge system.
- **Mauri:** life force.
- **Taonga:** those things and values that we treasure, both intangible and tangible.
- **Tapu**: sacred, restricted or prohibited.
- **Tikanga:** custom, rules.
- **Whakapapa:** genealogy.[1]

Identifying and addressing cultural impacts

First, organisations must make a reasonable effort to assess what the cultural impacts and effects on Māori could be. Then, consider whether and how to address them.

What this requires in practice will change depending on your specific use case and context.

[1] Kukutai, T., Campbell-Kamariera, K., Mead, A., Mikaere, K., Moses, C., Whitehead, J. & Cormack, D. (2023). Māori data governance model. Te Kāhui Raraunga

In general, we expect agencies to consider:

- Is it appropriate to specifically partner or engage with Māori whose information you intend to collect to gather their views? If so, who should you engage with – whanau/hapū/iwi, Māori individuals, Māori communities, all of the above?
- What is the risk of discrimination and bias against Māori from the use of the biometric system?
- Do you know what tikanga are engaged by your use of biometrics? Is your intended collection and use of biometrics consistent with those tikanga?
- Is your planned use of biometrics consistent with principles of Māori data sovereignty?
- Will Māori individuals/groups be involved in the ongoing co-governance, partnership, oversight or audit of your biometric system? If so, what representation from the people whose biometric information you are collecting will be necessary?

Once you have identified the potential cultural impacts and effects on Māori, if there are any negative impacts or effects, you need to consider whether and how to address those impacts. Some impacts or effects may not be able to be addressed. Failure to address those impacts or effects is a factor to be considered and may make the processing less proportionate.

If you do not have the internal expertise to make these assessments, you should consider whether it is appropriate to engage external advisers to provide cultural advice. The “further resources” section has links to other guidance which could assist you.

Do you need to collect ethnicity information to comply with this requirement?

You need to address cultural impacts whether or not you know specific ethnicity or cultural information about each impacted individual. In most cases, if you are undertaking biometric processing in New Zealand, it is very likely you will be collecting

Māori biometric information and so it is important that you consider what cultural impacts there may be.

In general, you do **not** need to collect ethnicity or cultural information to be able to consider potential cultural impacts. But, if you think you need to know how many Māori people may be impacted by your processing, you could consider using other metrics such as general population information to help you in your assessment.

Handling biometric information in accordance with tikanga

Collecting, storing and using biometric information in accordance with tikanga is one way of addressing cultural impacts and effects (but it is not the only way). Some starting points include:

- Ensuring that an individual's mana, mauri, hau, whakapapa and tapu is respected throughout the collection, use and disposal of biometric information.
- Considering the protection of Māori biometric information from a collective, rather than solely individual, perspective. In some cases, it may be appropriate **not** to privilege individual privacy at the expense of the collective benefit.
- Ensuring that biometric data of living individuals is not stored with biometric data of deceased individuals to protect their tapu.
- Holding Māori biometric information in New Zealand.
- Consideration of the concepts of utu (reciprocation) and ea (resolution or balance) in addressing any privacy breaches.

An example of a specific cultural concern for Māori is capturing images of moko and moko kauae (traditional facial tattoos), e.g. through a facial recognition system. Moko contain deeply sensitive and tapu information about an individual's identity such as whakapapa, whānau/hapū/iwi, whenua, ancestors and origins. Even if the biometric system does not specifically analyse the moko itself, the use or misuse of images that

include moko can affect the tapu, mana and mauri of the individual, and their whānau, hapū and iwi.

Free, prior and informed consent

Free, prior and informed consent is an important principle underlining Māori data sovereignty (principle: manaakitanga | reciprocity). Free, prior and informed consent involves agreement from the individual to the collection and use of their biometric information based on adequate information, appropriate timing and an absence of coercion. It gives people a genuine choice and autonomy over their information.

There must be a genuine alternative available to individuals to access for consent to be considered free, prior and informed. If there is no alternative, then individuals cannot freely consent.

In many cases, if you can gain the free, prior and informed consent of individuals before collecting their biometric information, this will be a valuable way to mitigate any negative cultural impacts.

Consent that doesn't meet the standard of free, prior and informed should be balanced by strong governance arrangements (partnership, oversight, and/or accountability mechanisms).

While free, prior and informed consent is not a mandatory part of the Code (and will not be appropriate or feasible for all circumstances), if it is an option for your specific use case, it is a good way to address cultural impacts.

Choose the right technology and processes to avoid bias

Bias in a biometric system is critical to identify and address to avoid negative impacts on Māori. Bias can enter the biometric system in different ways, from technical bias (i.e. repeatable errors produced by algorithm making a comparison or inference) to human bias (e.g. assumptions or judgements by people acting on the results). Mitigations include:

- Due diligence when choosing your technology or biometrics provider

- Testing and/or auditing results
- Putting processes in place to check unconscious bias
- Ability for people to challenge and/or correct results

Protecting children and young people

Take particular care when using a biometric system that may put the privacy rights of tamariki or rangatahi at risk e.g. adding them to a watchlist. In Mātauranga Māori, children are highly valued and considered taonga with inherent mana. They are a significant whakapapa link to the past and future. There is a strong imperative to minimise collection of their biometric information as they are more vulnerable to harms. In addition, breaches of privacy can affect whānau trust in government, business and systems.

Resources

The following resources are a starting point for agencies to learn more about Māori perspectives on privacy and build capability in this area:

- Publications by Tikanga in Technology research group, available at: https://www.waikato.ac.nz/research/institutes-centres-entities/institutes/te-ngira/research/tikanga-in-technology/indigenous-data-and-governance/
- He Poutama – Tikanga Māori in Aotearoa New Zealand law by the New Zealand Law Commission, available at: https://www.lawcom.govt.nz/our-work/tikanga-maori/tab/overview
- Kukutai, T., Campbell-Kamariera, K., Mead, A., Mikaere, K., Moses, C., Whitehead, J. & Cormack, D. (2023). Māori data governance model. Te Kāhui Raraunga. Available at: https://www.temanararaunga.maori.nz/nga-rauemi
- Guidelines for engagement with Māori from Te Arawhiti – the Office for Māori Crown Relations, available at: https://whakatau.govt.nz/assets/Tools-and-Resources/Crown-engagement-with-Maori-Framework.pdf

- Crown engagement with Māori guidance from Te Arawhiti – the Office for Māori Crown Relations, available at: https://whakatau.govt.nz/assets/Tools-and-Resources/Guidelines-for-engagement-with-Maori.pdf
- Khylee Quince and Jayden Houghton "Privacy and Māori Concepts" in Nikki Chamberlain and Stephen Penk (eds) *Privacy Law in New Zealand* (Thomson Reuters, Wellington, 2023).
- Hirini Moko-Mead *Tikanga Māori* (Huia, New York, 2013).

Rule 1 Example Scenarios

Note: All the examples in the guidance are simplified and are for illustrative purposes only. They are not an endorsement of any particular biometric system or a comment on any particular purpose or use case. Agencies must conduct their own assessment based on their own circumstances for each use of biometrics. Agencies will require more detail for their assessment than is included in the examples. Examples for each rule focus only on that rule and do not address compliance with all other aspects of the Code.

Facial recognition in a retail store – necessary and proportionate

A store wants to use FRT to identify individuals on a watchlist to help improve staff and customer safety and prevent shoplifting.

Assessment against rule 1	
Lawful purpose	The store has two lawful purposes: 1. To improve staff and customer safety. 2. To reduce shoplifting, particularly shoplifting of high-value items.
How the system will operate	Cameras will be mounted at key areas within the store. All people entering the store will be scanned. Non-match information and images will be deleted immediately. If there is a positive match

	with an individual on the watchlist, two staff members will confirm whether the positive match is correct (i.e. it has correctly identified a person on the watchlist) and then decide whether and what action to take. When establishing the watchlist, the store will only enrol people based on clear evidence of harmful behaviour such as previous aggressive or threatening actions towards staff members, other customers or store property, or having engaged in repeated, high-value shoplifting.

Necessary	The store determines the biometric processing is necessary because:
	• **Effectiveness:** The store assesses that the processing will be effective in achieving its stated purposes:
	  ○ Evidence from comparable retail stores domestically and overseas that have used FRT to improve staff and customer safety and prevent high-value shoplifting.
	  ○ Performance metrics, including accuracy rates, from the provider of the biometric system.
	  ○ Information about the training or evaluation data that the provider used, compared with the demographics of customers of the store.
	• **Alternative means:** The store considers what alternatives there could be for achieving its purpose(s), including:
	  ○ Employing security guards.
	  ○ Additional obvious security cameras (CCTV).
	  ○ Physical measures to reduce shoplifting such as security tags on high-value items.

	After assessing the alternatives, the store determines that its lawful purpose cannot reasonably be achieved as effectively by an alternative with less privacy risk. That is because the store has already invested in some additional security measures like security tags and additional CCTV, but these measures have not had a sufficient impact on the rate of harmful behaviour or repeated, high-value shoplifting.
Safeguards	The safeguards the store adopts to reduce privacy risk include: • Thorough testing of the FRT system before deployment. • Deleting images and non-match information immediately. • Using best practice security measures (see rule 5). • Ensuring there is appropriate and adequate staff training for all staff involved in watchlist enrolment decisions and any responses to FRT alerts.
Proportionate	The store believes on reasonable grounds that the biometric processing is proportionate.
• **Risk assessment**	• High level of inherent intrusiveness: the FRT system is operating live, in a semi/quasi-public space. All people entering the store have their faces scanned, sometimes multiple times as they move through the store. o Mitigation: automatic and immediate deletion of non-match images significantly means that most images are not retained and cannot be reused for another purpose. • An element of surveillance risk. Use of live FRT in a semi/quasi-public space reduces the ability of individuals to avoid being monitored. However, this store is not considered an essential service (operating FRT in an

	essential service would increase the overall level of privacy risk as people have a reduced ability to choose not to visit that store). • Potential risk that individuals will be misidentified and could suffer harm as a result. • Risk around lack of awareness. Although there will be signs, it is likely some customers will not notice or understand these and be unaware of the operation of FRT. • Possible chilling effect. Some individuals may also be deterred from exercising their freedom of movement because of the FRT (notwithstanding that images of people not on the watchlist will be deleted immediately). • Some risks around accuracy. The watchlist will need to be carefully managed to ensure that enrolment images are good quality and that the criteria for adding and removing people from the watchlist are followed. A poorly managed watchlist may also exacerbate risks of over surveillance, chilling effects and breach other data protections such as scope creep (including children's information on watchlist). • Possible storage and security risks: There's a low risk the watchlist or biometric system may be accessed by unauthorised staff and misused. Immediate deletion of non-match images reduces the information stored and therefore meaningfully reduces this risk. **Outcome of risk assessment:** Substantial risk mitigated by appropriate safeguards.

• **Benefits weighed against risks**	• **Benefit of using FRT for safety**: reduction in violence, aggression and threats made against staff and customers and safer workplace for staff (public benefit). Based on similar case studies and its assessment of effectiveness, the store expects statistically significant and meaningful reduction. • **Benefit of using FRT to reduce shoplifting:** reduction in stock loss by the store, better use of staff time, and increased revenue (private benefit). Although there may also be some general public benefit from lower shoplifting in the sense of reduced crime, the primary benefit from reduced shoplifting is the private benefit to the store. **Weighing benefit against risks** • **Using FRT for safety (public benefit)**: In accordance with rule 1(4)(a), the store considers that, with the identified safeguards reducing the level of risk, the benefit of using FRT **outweighs** the residual privacy risk. • **Using FRT to address shoplifting (private benefit)**: After weighing the benefit and risk in line with rule 1(3)(c), the store considers that the benefit to the organisation from using FRT to address high value shoplifting events and prolific shoplifters **outweighs** the privacy risk **by a substantial degree**. o However, the store considers that the advantages of using FRT to address low-value or one-off shoplifting events does not outweigh the associated

	privacy risk by a significant margin and won't meet the test in rule 1(3)(c). o Accordingly, the watchlist criteria would need to be focused on safety concerns and high value or repeated shoplifting only.
• **Impacts on Māori**	• One possible impact on Māori that the retail store considers is the possibility of lower accuracy for Māori customers, or bias (unconscious or conscious) in staff members responsible for the watchlist. This could lead to discrimination against Māori customers either through misidentification or unwarranted enrolment on the watchlist. • The retail store plans to mitigate this impact by choosing a FRT system with high accuracy across all relevant demographic groups, requiring clear and objective criteria to be meet before enrolling someone on the watchlist, ensuring staff members receive training on bias and discrimination and actively monitoring the system for unexpected results once in place.
Overall conclusion	Overall, the collection is necessary for a lawful purpose, proportionate and reasonable safeguards will be implemented.

Facial recognition to facilitate payment in school cafeteria – not necessary and not proportionate

A school plans to install a FRT system to allow for cash and card-free payment at the school cafeteria.

Note: this scenario is similar to case reports from the UK Information Commissioner's Office. For more information, see the ICO website.

Assessment against rule 1	
Lawful purpose	The purpose is to facilitate cashless payments at the cafeteria.
How the system will operate	The school will install cameras at the payment point in the school cafeteria where live FRT will be used to identify the child purchasing food at sale point and deduct the meal price from their prepaid school lunch account.
Necessary	After assessing the effectiveness and available alternatives, the school thinks that the biometric processing is probably **not necessary** to achieve their purpose. • **Effectiveness:** After assessing the data from the FRT provider and considering a case study in the setting of a workplace cafeteria, the school determines that FRT could be an effective way to offer a cashless payment method. However, there could be some accuracy issues as the children at the school grow and their faces change. • **Alternative means:** There are many alternative ways of meeting the lawful purpose of facilitating a cashless payment system that would be significantly less privacy intrusive and likely just as effective. For example, by having physical tokens, a swipe card or entering the student's ID number at point of sale. This is particularly the case given the privacy risks associated with the collection of children's biometric information (see the risk section below).

	Overall, it is not clear that the biometric processing is necessary. Because it is not necessary, collection would not be permitted under rule 1. However, the school also considered the proportionality of the collection.
Safeguards	• Images from the FRT system would be deleted after one billing cycle (to enable parents to challenge any possible misidentifications leading to incorrect charges). • There would be a governance committee to oversee the FRT system. • The school would choose a system that has a high degree of accuracy for young people. • The school would engage a technical expert to assist with establishing security safeguards for the biometric information stored, such as encryption and other technical protections. • The school considers seeking parental authorisation, but determines in their setting it would be practically difficult to prevent the cameras from capturing any information of people who have not authorised the collection. This means that authorisation cannot be relied on as an effective safeguard in this context if all people who enter the cafeteria have their biometric information collected, whether or not they have authorised it.
Proportionate	The school determines that the biometric processing would **not be proportionate.**
• **Risk assessment**	• Children are a more vulnerable population. Children generally have a lower ability to appreciate the risks or envisage the consequences associated with the processing of their biometric information. They also may

	not be as aware of their privacy rights and may have more difficulty exercising them. • There is a significant power imbalance between the children and the school and some power imbalance between the children's parents and the school. If no genuine alternative is offered, the potential negative impact of the power imbalance is heightened. • There is a risk of misidentification or errors which could lead to financial consequences for individuals (incorrect billing of food items) or embarrassment for a child that cannot pay. • The school would likely need to retain images from the FRT for a set period to enable parents or students to challenge any suspected incorrect bills. Storing information increases privacy risk. • There may be particular psychological harms for children from the normalisation of surveillance in their everyday lives. For example, children are more vulnerable to the negative impacts of surveillance, including lack of trust, changing the nature of interactions with others and authority, denying children experiences, and incentivising secrecy and subversion. • A review of the school's own privacy and security maturity shows that it does not have sufficient expertise internally to manage the system safely on an ongoing basis. **Outcome of risk assessment:** Significant risk that is not sufficiently mitigated by safeguards.

• **Benefits weighed against risks**	Increased efficiency of payment in the cafeteria and a reduction in the need for cash to be carried at school. This is a benefit to the school so it would need to substantially outweigh the privacy risk. **Weighing benefit against risks** • The increased convenience does not substantially outweigh the privacy risk.
• **Impacts on Māori**	• Possibility of lower accuracy for Māori students, leading to higher rates of misidentification. • School needs to consider tikanga of collecting information of tamariki.
Overall conclusion	Overall, the biometric processing is **not** proportionate. There is insufficient benefit to justify the high privacy risk.

Fingerprint scan for Multi Factor Authentication (MFA) – necessary and proportionate

An organisation has highly sensitive information that only a limited number of employees need access to, currently protected by multi factor authentication (MFA) using a combination of password and mobile-based factors. Because of the highly sensitive nature of the information, the organisation plans to enhance security by moving to a biometric authenticator (fingerprint recognition) in place of the mobile-based factor.

Assessment against rule 1	
Lawful purpose	To protect a database of sensitive information.
How the system will operate	The organisation will consult with its employees about the need for increased security and possible biometric authenticator, allowing employees to raise concerns and/or ask questions. If it

	decides to go ahead with fingerprint MFA, then employees will be required to enrol a fingerprint sample using the fingerprint reader on their work laptops and subsequently scan in to access to the information. If an employee chooses not to provide a sample, they will no longer be permitted to access the information, which could require redeployment into another role.

Necessary	The organisation believes the biometric authentication factor is necessary:
	• **Effectiveness:** the employer believes the fingerprint verification system will be effective based on:
	  ○ Performance metrics from the provider of the biometric system (false acceptance and rejection rates, equal error rates, presentation attack detection, time taken to verify).
	  ○ Evidence about the technical validity of overall process to enhance security.
	• **Alternative means:** There are other authentication factors that the employer could use, including both different biometric factors (e.g. iris scanning) and non-biometric factors (e.g. SMS code, smart cards). The organisation considers that, for its context, the fingerprint authenticator has advantages over the other non-biometric options, including being resistant to phishing attacks, unable to be lost or forgotten and unlikely to be stolen. It is also more practical to implement than other biometric options like iris scanning or facial recognition and doesn't present accuracy differentials across demographic groups. Overall, there is no reasonable alternative that would

	enhance security as effectively and also poses less privacy risk.
Safeguards	• Consultation with affected employees and commitment to work with employees to resolve or mitigate any concerns raised by employees. • Only retain a template of the fingerprint scan, not the actual sample, to reduce risks of spoofing and presentation attacks. • Best practice security measures to protect the biometric information in the context, including storing locally on device.
Proportionate	The organisation believes on reasonable grounds that the biometric processing is proportionate.
• **Risk assessment**	**Risk assessment:** *Factors contributing to lower risk:* • Limited scope: targeted and minimal biometric information collection measure, from only those who need to access the sensitive information. • Strong technical safeguards to protect the biometric information. *Factors contributing to higher risk:* • Power imbalance: The inherent power dynamic of the employment relationship increases the intrusiveness of the measure as employees may feel they have a lack of choice in giving their biometric information. This is particularly the case, if they cannot do their job without accessing the sensitive information and will have to change roles.

	○ Mitigation: Consulting with employees and offering the choice to opt-out (a limited opt out due to consequence of redeployment) provides some degree of mitigation against the power imbalance. **Outcome of risk assessment:** Overall low risk
• **Benefits weighed against risks**	• **Benefit:** The increased level of security benefits the organisation (private benefit) by preventing data breaches and unauthorised access, ensures compliance with any legal requirements around security, protects the organisation's reputation, ensures client trust, and reduces financial and operational risks. This benefit substantially outweighs the risk.
• **Impacts on Māori**	• As part of the consultation with employees, the employer will specifically seek feedback on cultural impacts from Māori employees and consider how to address any impacts raised. • The fingerprint recognition technology used has a high accuracy metrics that do not differ across demographic groups. • The fingerprints will be stored locally on each individual's laptop so no biometric information will leave New Zealand (better reflecting Māori data sovereignty principles).
Overall conclusion	Overall, the collection is necessary for a lawful purpose, proportionate and reasonable safeguards will be implemented.

Voice sample and behavioural biometrics – necessary and proportionate

A bank plans to use biometrics systems to verify customers for fraud detection and prevention purposes.

Assessment against rule 1	
Lawful purpose	Ensuring customer accounts are only being accessed by the correct customer to detect and prevent fraud.
How the system will operate	The bank will set up a voice verification system that collects voice samples to verify customers over the phone when they call the bank. The bank will also collect behavioural information based on how the customer interacts with the mobile app and website such as keystroke logging and mouse and finger movements. This information will be used to create a profile of the customer's use patterns, continuously authenticate them as they access their account and generate an alert if there is a noticeable change in behaviour that could indicate fraud.

Necessary	The bank assesses that the voice and behavioural verification systems are necessary:
	• **Effectiveness:**
	  ○ Performance metrics from the providers of the voice and behavioural verification systems.
	  ○ Evidence about the technical validity of the overall process and any weaknesses or disadvantages.
	  ○ Review of comparable use domestically or in overseas jurisdiction.
	  ○ Results from testing the systems before live rollout.
	• **Alternative means:** The bank considers other over-the-phone verification methods, such as security questions, are insufficiently effective to verify customers. They are

	vulnerable to social engineering attacks and, in fact, pose greater privacy risk than voice verification due to relying on more easily accessible personal information.
Safeguards	Some of the safeguards which are relevant and could help reduce privacy risk are: • High level of transparency with bank customers about what information is collected. • Thorough testing of the systems before deployment. • Using best practice security measures to protect stored biometric information. • Robust operational safeguards including access limits and retention policies.
Proportionate	The bank assesses that the biometric verification systems are overall proportionate.
• **Risk assessment**	**Risk assessment:** *Factors contributing to increased risk* • Lack of control / choice: customers can't opt-out of the collection of their biometric information (because that would be detrimental to the purpose of preventing fraud). • Lack of transparency: behavioural and voice biometrics can be collected passively without the customers' awareness of what information is being collected, why and how its being used. • Profiling / scope creep: continuous collection of behavioural biometrics enables a profile of the customer to be created which can reveal other sensitive traits like cognitive or physical impairments. Voice samples can also reveal other sensitive information about the individual.

	Factors contributing to lower risk • Minimal to no risk of impact on other protected rights. **Outcome of risk assessment:** Some risk, largely mitigated by safeguards.
• **Benefits weighed against risks**	• **Benefit:** increase in security of customers bank accounts and reduction in fraud and misuse. This has a clear benefit to the individual, as well as a benefitting the bank. The clear benefit to the customer – enhanced account protection and reduced risk of fraud – justifies the customers lack of ability to avoid the collection of their biometric information and minimal risk of scope creep.
• **Impacts on Māori**	• The bank ensures the voice biometrics will be accurate for Māori, including if Māori customers are speaking te reo Māori. • The verification systems require approval and oversight by a governance board that has Māori representation.
Overall conclusion	Overall, the collection is necessary for a lawful purpose, proportionate and reasonable safeguards will be implemented.

Running a trial under the Code

Rule 1 (and rule 10) allows organisations to establish a trial to assess whether their proposed use of biometrics for a particular purpose is going to be **effective**.

Being able to show that your collection and use of biometric information is effective, and therefore necessary to achieve your purpose is required in rule 1.

Before the trial

Do I need to run a trial? When should I run a trial?

It is not compulsory to run a trial. Running a trial may be appropriate if you can comply with all other parts of the Code but you need more evidence to determine whether your collection or use is effective.

If you have enough evidence to assess the effectiveness of your proposed processing, then the Code does **not** allow you to run a trial. See the guidance on what evidence can show effectiveness for more information.

Running a trial **only** allows compliance with the **necessity** test to be deferred until the end of the trial period. You should not establish a trial unless you can comply with all parts of the Code except the necessity test – all other parts of the Code must be complied with during the trial.

Is a trial the same as testing your biometric system?

A trial is different from testing your biometric system. A trial is used to evaluate real-world effectiveness. A test is a practice procedure carried out in a controlled environment to identify specific issues or assess if the system behaves as anticipated (without taking real-world actions).

Staff training

Any staff involved in operating or using your biometric system during the trial will need to receive appropriate training and supervision before the trial, and during the trial as necessary.

During the trial

How long can I run a trial for?

A trial must not run for any longer than is necessary to give you sufficient information about the system's effectiveness and enable you to compare the biometric systems against any lower risk alternative solutions. Before establishing the trial, you need to notify how long the trial will go for.

There is no minimum period for a trial, but the maximum time for a trial is an initial period of 6 months, with a possible extension of a further 6 months if you have not established effectiveness by the end of the initial period (overall, not longer than 1 year).

If you cannot demonstrate that your biometric processing is effective by the end of the trial period (including the extension, if relevant), then you have **not** met the effectiveness requirement and you must stop collecting or using biometric information.

Can I make changes to the biometric system while running a trial?

The primary purpose of the biometric processing and the core way it is used during the trial should be the same as the intended use after the trial. But you can and should make changes during your trial to make improvements to safeguards and reduce the privacy risk, improve accuracy and performance of the system, and respond to feedback from users and individuals whose information is collected.

Do I need to tell people about the trial?

You need to comply with all the rule 3 requirements. This includes telling people about the fact that you are collecting biometric information during a trial and how long your trial period is for.

Can I take actions that may impact people during a trial?

You should consider whether it is appropriate to take adverse actions against individuals during a trial. An adverse action is an action you take that could negatively impact the individual, for example, removing them from your premises, monitoring their behaviour or imposing a fine on them

In some cases (e.g. fraud detection), it may not be possible to gain the necessary evidence from your trial without taking actions that negatively impact people. But, if it will not undermine the purpose of the trial period, you should consider not taking any adverse actions against individuals during the trial period.

If you are taking actions that may affect people during the trial, you should also tell people about that, unless doing so would undermine the purpose of the trial or the actions.

Privacy harm or non-compliance with the Code during a trial

OPC can still investigate any complaint brought by an individual about a breach of one of the rules in the Code (or the principles in the Privacy Act) or otherwise use our compliance powers under the Privacy Act during a trial period. You must notify OPC of serious privacy breaches during the trial, including by any of your agents or service providers, in accordance with the Privacy Act. You are also accountable to people for any privacy harm caused to them during a trial period.

When a trial ends

Assessing effectiveness and alternatives

Use the evidence gathered from your trial to assess whether the biometric processing was effective in achieving your lawful purpose and whether you could reasonably achieve your purpose **as effectively** using an alternative option that poses less privacy risk.

To meet the effectiveness requirement, there needs to be a clear and direct link between the biometric processing and achieving your purpose. If you could achieve your purpose easily without the biometric processing, then the biometric processing will not be necessary. See the effectiveness guidance for more detail.

Assessing the effectiveness of the processing during the trial will also help you determine whether there is a reasonable alternative available to the biometric processing.

If your assessment shows that the processing was **not effective** (or not sufficiently effective) or that there **is** a **reasonable and effective alternative** with less privacy risk, then you have not met the necessity requirement in the Code and you must stop collecting or using biometric information for your purpose.

However, if your assessment shows that the processing **was effective**, and that there is **no reasonable and effective alternative** with less privacy risk, then it may be appropriate to continue collecting or using biometric information for your purpose, provided you can continue to comply with the other requirements in the Code.

If you need time to complete the assessment about effectiveness, stop collecting or using biometric information until such time as you have determined that the processing was effective, and that there is no reasonable and effective alternative with less privacy risk.

What should I do with information collected or used during a trial?

When your trial period comes to an end, you need to consider what to do with the biometric information you collected or used. Rule 9 requires that you only keep information for as long as required for the purposes for which it may lawfully be used.

If your trial did not provide you with sufficient evidence that the processing is necessary (e.g. it was either not effective or there was a reasonable and effective alternative available), then you need to consider whether you continue to have a lawful purpose for holding the information, and, if not, you will need to securely destroy it. It could be that you have a lawful purpose for retaining some of the information – e.g. retaining some samples or the data used in your evaluation – but not other information – e.g. destroying templates if you will no longer be using them. You will also generally need to retain any information that is the subject of a privacy complaint or compliance action.

If your trial showed that the biometric processing is necessary and effective for your purpose, and you intend to continue biometric processing on an ongoing basis, then it may be appropriate to retain information that you collected during the trial and continue to use it, if you are confident that the trial information is suitable for your ongoing biometric processing.

You will need to carefully assess whether it is appropriate in your circumstances to retain information you collected or used during a trial, or whether you will securely

destroy it and then collect new information after the trial. As part of your decision, you will need to consider what you told individuals when you collected their information and how your trial was set up and run. You should also consider whether you are making any changes (e.g. to system settings, safeguards or other protections for information) that could mean you should securely destroy information collected during the trial (e.g. if you have changed settings that would justify deleting biometric templates and regenerating them according to a higher quality standard.)

Rule 2: Collect biometric samples directly from the person

Rule 2 of the Code is about where you collect biometric samples from (image of face, voice recording, fingerprint scan etc.). Unless an exception applies, you must only collect biometric samples directly from the person whose information it is.

Collect biometric information directly from the individual

Collecting biometric samples directly means that the source of the sample is the person whose information it is. Direct collection helps improve transparency, gives the individual more control over their information, and will often mean that the information you collect is most accurate and up to date.

The individual does not need to be aware of the collection for it to be direct (but see rule 3 for notice requirements).

Using a third-party to collect biometric samples directly from the individual on your behalf will still be direct collection. See our guidance on working with third-party providers for more information.

Direct collection could look like:

- The individual sends you a photograph of themself to enrol in your facial recognition system.
- You take a fingerprint scan from someone to use in a security access system.

- You collect a voice recording from a customer when they call your call centre for fraud detection and prevention purposes.
- You collect stills of people's faces from your CCTV system to use in a facial recognition system.
- You use a hidden facial recognition camera to collect biometric samples for law enforcement purposes. Even though the individual may not be aware that their biometric sample is being collected, you are still collecting it directly from the individual.

Collection that is **not** direct could look like:

- Another business shares their database of facial images of customers and you use the database for your facial recognition system.
- You obtain a biometric sample of your employee from their former employer.

What if you delete the biometric information quickly?

"Collect" means to take any step to seek or obtain the information. Even if you delete the information quickly, you are collecting the information if you hold the information even for only a fraction of a second. But deleting the information quickly can be an important safeguard that helps you comply with other rules in the Code.

Exceptions: When you can collect biometric information from other sources

You can collect a biometric sample from someone other than the individual if you believe, on reasonable grounds, that one of the below exceptions applies.

What does believe on reasonable grounds mean?

A reasonable belief requires more than just suspecting something might be the case – you must have some evidence for why you think an exception applies. You should keep a written record of why you believe the exception applies.

You must consider whether the exception applies each time you collect biometric samples and whether it applies to everyone whose information you are collecting.

If you aren't sure whether an exception applies, you must not rely on that exception. If no exception applies, you must either collect the information directly from the individual or not collect the information at all. Sometimes, more than one exception may apply to your situation. You should still record the reasons for relying on each exception.

Some of the rule 2 exceptions (for example, avoiding prejudice to the maintenance of the law), are also exceptions in other rules. The same general guidance for those exceptions applies to the exception in each rule.

Exception	Note on when the exception applies
Collecting the information directly from the individual would be prejudicial to the individual's interests. **Note:** This exception in the Code has a **higher standard** than the similar exception in IPP 2. In the Code, this exception only applies if collecting the information directly from the individual would be actively prejudicial to their interests.	Exception may apply when: • You know that someone would be harmed if you collected the biometric sample directly from them. For example, someone has a health condition that means it would be harmful to collect the biometric sample directly from them. • The individual cannot provide the sample directly or authorise the collection, but the individual could be adversely affected if the sample is not collected and processed for their benefit. Exception would not apply when: • You assume it would be prejudicial to the individual's interests, but you don't have any good evidence about why. Note: You should consider asking the individual for their view about whether collecting information directly

Exception	Note on when the exception applies
	from them would be prejudicial to their interests. Asking the individual will not always be appropriate – for example, if it would be detrimental to their mental health. But, particularly where it would be more costly or inconvenient for them, you should generally seek individual authorisation to collect the information from another source, rather than rely on the "prejudicial to the individual's interests" exception. Some individuals may prefer to provide information directly, even if it is more inconvenient for them.
You would not be able to achieve the purpose for collecting the biometric information if you collected the information directly from the individual.	Exception may apply when: • You are collecting biometric samples for fraud investigation and collecting the information directly from the individual would undermine your investigation. Exception would not apply when: • It is less convenient for you to collect the information directly from the individual, so you don't want to.

Exception	Note on when the exception applies
The individual authorises the collection from someone else.	Exception may apply when: • You've given the individual all the information they need to understand the collection of their biometric sample in the specific circumstances, and they authorise you to collect the biometric sample from someone else. Exception would not apply when: • You haven't explained all the information the individual needs to know – for example, you didn't explain who you will collect the biometric sample from, or what kind of biometric sample you will collect. • You pressure, coerce or threaten the individual into authorising the collection.
The information is publicly available.	Exception may apply when: • You are collecting a biometric sample from a publication such as a book, newspaper, or public register. • You are collecting a biometric sample from a website or public social media page e.g. a public profile picture. Exception would not apply when: • You are collecting a biometric sample from photos on social media that require you to have additional

Exception	Note on when the exception applies
	permission to view the photos (such as being a friend or a follower of the social media account). • The information is only public because of a privacy breach (and you know, ought to know or reasonably suspect that this is the case).
It is necessary to avoid prejudice to maintaining the law (including in relation to court proceedings), enforce specific laws, or protect public revenue.	Exception may apply when: • A public sector agency is investigating an offence and needs to collect a biometric sample from someone else to adequately investigate the offence, and the agency has followed all other relevant laws that apply to obtaining evidence. • You are not a law enforcement agency, but you have an urgent or exceptional situation, where it is necessary to collect a biometric sample from another source for biometric processing to avoid a likely risk that a relevant law enforcement agency function would be prejudiced (e.g. to be able investigate serious offending). (Note – this will be rare because there are likely other rule 2 exceptions that you can use when you set up the purpose for your biometric processing.) Exception would not apply when: • You are not a law enforcement agency, but you want to obtain a biometric sample from someone else to do your own investigation of a suspected offence. (Note – if investigating suspected

Exception	Note on when the exception applies
	offending is the purpose of your biometric processing that meets rule 1, then you can likely use other exceptions under rule 2).
It is necessary to prevent or lessen a serious threat to someone's life or health	Exception may apply when: • There is a real and serious threat to any person's life or health, and collecting a biometric sample from someone other than the individual concerned for the purpose of biometric processing will help you prevent or lessen that threat. Exception would not apply when: • There is a serious threat to a person's life or health, but collecting the biometric sample will not help prevent or lessen that threat. Also see our further guidance on this exception in the Privacy Act.
The overall circumstances mean you cannot comply with rule 2 for the particular case.	Exception may apply when: • There is a legitimate and unavoidable reason why you cannot comply with rule 2 in the particular circumstances, and no other exception applies (for example, you cannot seek individual authorisation).

Exception	Note on when the exception applies
	Exception would not apply when: • You could reasonably change the circumstances to make it possible to comply with rule 2 in the particular case.
The individual will not be identified when the information is used, or the biometric information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.	Exception may apply when: • You are using biometric information as part of a research study and only aggregated information that will not identify anyone will be published. Exception would not apply when: • You have removed someone's name or their face from their biometric information, but they can still be identified in other ways. • The audience of a publication may have additional knowledge to help them identify an individual in the research. We have more guidance on what makes a personal identifiable. While you can rely on an exception to rule 2 in these circumstances, if you are using biometric information for statistical or research purposes, it will usually be good practice to still collect information directly from the individual where possible.

Rule 2 Example Scenarios

Facial recognition in a gaming venue

Topics covered: direct collection would be prejudicial to the individual's interests, not reasonably practicable to collect the information directly from the individual.

The Gambling Act places a duty on venue managers to assist problem gamblers, including by issuing an exclusion order under the Gambling Act in some circumstances. A gaming venue plans to use FRT to help enforce exclusion orders under the Gambling Act. It will use stills from the video footage captured by the venue's existing CCTV system if the quality is high enough (direct collection).

If the venue does not have an existing sample that is high enough quality to use, it may ask the individual for a photo to include (direct collection).

The venue considers any indirect collection on a case-by-case basis. Some situations that could justify indirect collection are:

- The individual cannot provide a suitable photo and the venue believes that asking the individual to come to the site to take a photo to use in the facial recognition system could cause them harm by triggering a desire to gamble. In this case, direct collection would be detrimental to the individual's interests.
- The venue has received notice of a venue-initiated exclusion order from another venue, and based on the information received, it has reasonable grounds to believe that the relevant individual would refuse to provide a photo. Therefore, the venue decides to collect a photo from another gaming venue (indirect collection) because collecting it directly from the individual would prejudice the purpose for collection.

Fingerprint scan for Multi Factor Authentication (MFA)

Topics covered: Using a third-party provider.

A business has access to highly sensitive information. It wants to ensure only the correct staff members have access to a limited, highly restricted database. It decides to implement a multi-factor authentication system using employee fingerprints.

Most employees are based in the business's main office. The employer decides to collect employee fingerprints directly in the main office on certain days.

A few employees work remotely. The business gives its remote employees the option between travelling to the main office or having their fingerprint samples taken by a third-party provider. Using a third-party provider in this way is still considered direct collection by the business.

Collection of voice sample and behavioural biometric information

Topics covered: Direct collection, fraud prevention.

A bank uses a voice recognition system for customer phone calls and also collects behavioural information based on how the customer interacts with the mobile app and website e.g. keystroke logging and mouse and finger movements. This information is used to create a customer profile and generate an alert if there is a noticeable change in voice or behaviour that could indicate fraud. This information is collected directly from customers when they interact with the bank.

Rule 3: Tell people about the information you collect

Rule 3 is about being open with people about why you are collecting their biometric information and what you will do with it.

What you need to tell people

There are several things you need to tell people if you are collecting biometric information. You need to take the steps that are reasonable in your circumstances to make people aware of the matters below. That means that you can take account of the type of interaction and relationship that you have with affected individuals.

What you need to tell people	Guidance or example
The fact that biometric information is being collected.	Tell people you are collecting biometric information and specify exactly what kind of information you are collecting. Consider expressing it in non-technical terms if this will help people understand e.g. say “a scan of your fingerprint” not “a biometric sample”
Each specific purpose for which the biometric information is being collected.	Tell people why you are collecting their information. Your purpose should be specific enough so the individual can understand what their information is being used for e.g. “to detect when individuals on a watchlist enter our premises and monitor their actions”, not “for business use” or “for general security”.

What you need to tell people	Guidance or example
If there is an alternative option that is available.	Be clear on how people can access the alternative process. Ensure the information about the alternative is clearly visible and accessible. You only need to tell people about any alternative option that you actually have available to use – not any possible alternative you may have considered as part of your rule 1 assessment. For example, if people can use a swipe card instead of FRT to access a site, tell people this and tell them how to access the alternative option.
The intended recipients of the biometric information.	Let people know who will have access to their biometric information. For example, if you are collecting information on behalf of someone else or you have an obligation or reason to share the information with someone outside your organisation who will use the biometric information for their own purposes.
The name and address of who will collect and hold the biometric information.	Give people the contact details that you would like them to use if they have any questions about biometric information.

What you need to tell people	Guidance or example
If there is a specific law that requires or allows you to collect, use or disclose the biometric information, what that law is and whether the individual has a choice to provide the information.	If there are multiple laws that could apply, you can just list the most relevant law. Laws that apply can include New Zealand law (including an authorised information sharing agreement), or the laws of another country.
What happens if the person doesn't provide their biometric information.	E.g. will they immediately lose access to services? Will it be all services or just some? Will they have to provide other information?
That the person has a right to request to access and correct their biometric information, and that people have the right to complain to the Privacy Commissioner about any action that the Code applies to.	See our rule 6 and rule 7 guidance for more information about access and correction requests. Information about submitting a complaint is available on our website.
A summary of your retention policy for biometric information.	Provide information about how long you will keep the person's biometric information for. This could be a time period (e.g. 5 years to meet a specific legal obligation) or what circumstances trigger deletion (e.g. if a customer requests to delete their account).
How the person can raise a concern or complain about how their biometric information is handled	If you expect people to follow a particular process to raise a concern or complain to you (e.g. using a specific form), you should make that process easily available to them.

What you need to tell people	Guidance or example
If your proportionality assessment under Rule 1 is either publicly available or available on request, where and how the person can view it.	It is not mandatory to make your proportionality assessment publicly available or available on request, but it is good practice to do so, especially if you are a government agency or a provider of an essential service.
If you are running a trial, that you are running a trial and how long it will go for.	See our trial guidance for more information about running a trial.

When you need to tell people

Some matters in rule 3 must be conveyed to individuals **before** or **at the time** you collect biometric information. We call this the "minimum notification rule". The minimum notification rule matters are:

- 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.

For the minimum notification rule, you must communicate in a "**clear and conspicuous"** way. You must also include a location, address or other method for people to obtain further information about the biometric processing.

Clear and conspicuous

Clear and conspicuous means information should be obvious, accessible and easy to understand.

For example, you could:

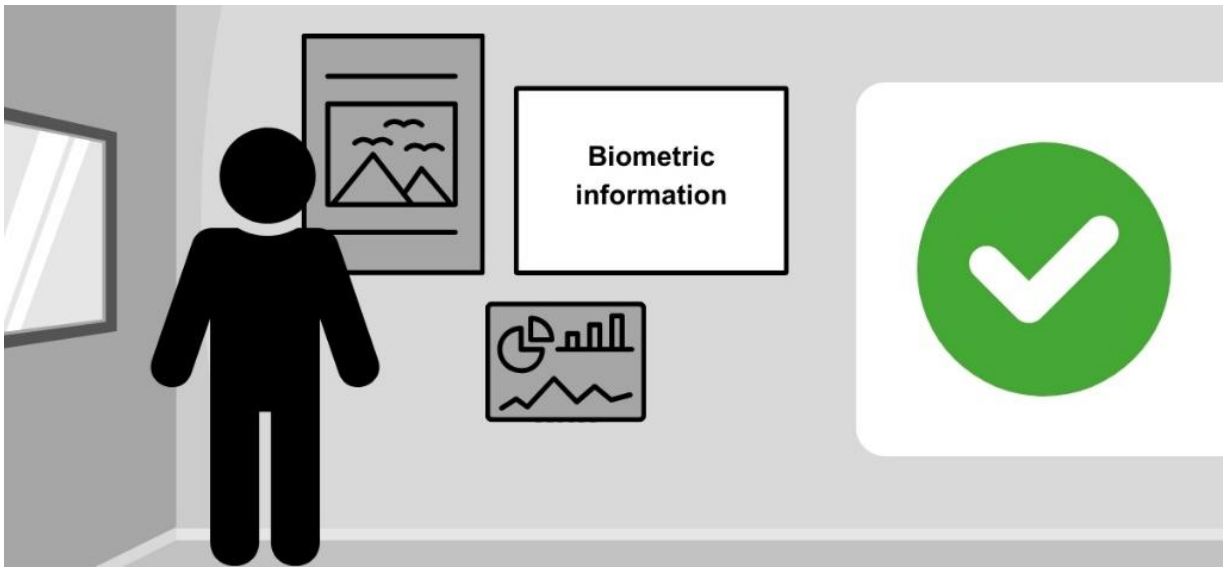
- Ensure any signs or website content are large enough to draw people's attention, easy to read, distinguishable from other signs e.g. promotional signs, and placed

apart from other signs so that the biometric information isn't lost among all the other information.

- Ensure verbal or audio notices (e.g. given by staff or prerecorded) are clear, easy to understand and that they let people know where they can access further information.
- Create a specific web page if there is a lot of information that needs to be provided, or place information under clear headings if it is part of a larger document.
- Require people to scroll through information before they can tick a box to confirm they have read it.

Example: Clear and conspicuous

Biometric information is set apart from other information (such as promotions) and is large enough to easily notice and read.



Example: Not clear and conspicuous

Biometric information is partially covered by or not sufficiently set apart from other information and is not large enough to easily notice and read.

For all other matters in rule 3, you must inform individuals of those matters **before collecting** their biometric information, or if that is not practicable, **as soon as practicable after collecting** their biometric information.

While it is not required that the other matters be communicated in a clear and conspicuous manner, you still need to take reasonable steps to ensure the individual is aware of the matters. This requires you to consider how the information is presented and communicated.

You may not need to tell people repeatedly

You do not have to inform an individual of the matters in rule 3 if:

- you have already informed them of the rule 3 matters on a recent previous occasion, and
- the information you are collecting is the same or the same kind of information (for example, you are collecting facial images for FRT on each occasion), and
- you are collecting it for the same purpose as the recent previous occasion.

What is considered a "recent previous occasion" will depend on the overall circumstances. How likely is it that the person may have forgotten about the collection of their biometric information and what their rights are? You should consider:

- **Are you enrolling a person in a biometric system or collecting their information subsequently?** Enrolling a person in a biometric system will warrant full notification but it may not be necessary on subsequent times the person uses that system e.g. an employer who has set up a MFA system that uses fingerprinting does not need to notify the employee each time the employee scans their fingerprint post enrolment.
- **How often do you collect biometric information from the person?** For example, if you are collecting the same biometric information from the same person for the same purpose every week, we don't expect that you to tell them about the rule 3 matters each time.
- **How are you telling people about the rule 3 matters?** If you are telling people through a one-on-one conversation with a staff member, this probably wouldn't

require as many reminders compared to using signage which should be continually present.

- **How is the biometric information collected?** Is it obvious each time biometric information is collected – e.g. the person scans their fingerprint or stands in front of a specific camera? In that case, it may be appropriate for there to be a longer period between when you inform the individual of the rule 3 matters. If it is less obvious to the individual each time their information is collected – e.g. the person simply has to enter a general area for their biometric information to be collected – then it will generally be appropriate to inform people more frequently.

In any case, if you change the information or kind of information you collect, or you change the purpose for which you are collecting the information, you will need to inform the individual of those changes.

The requirements in rule 3 are specific to each person whose information you collect. If you are not sure whether you have informed someone on a recent previous occasion (for example, because you do not collect a record of when you inform each person or because you do not know what is “recent” in your context), then you need to consider whether you should inform the person of all the rule 3 matters each time you collect their information.

Example: A business uses voice biometrics in its call centre to verify customer ID. The business informs all callers about the minimum notification rule matters at the start of the call, and then once the customer’s ID is verified, the call centre can assess whether the customer needs to be told about the other rule 3 matters, or whether they were informed on a recent previous occasion.

How to tell people

You must take reasonable steps to ensure individuals are aware of the matters outlined in rule 3. In general, we encourage you to:

- Use plain language. If you refer to technical concepts, you should explain them in a way someone without technical knowledge will be able to understand.
- Consider the accessibility of your content for people with disabilities.
- Consider the primary language of the people whose information you are collecting.
- Consider translating materials into other languages if necessary, especially if your use of biometrics is high risk and you know that many people will need translated materials to understand the information. See our guidance on rule 1 for more information on assessing risk.
- Consider how the information is presented visually – design, timing and placement of information can make a big difference to whether people will see it and understand it.
- If you are providing information to people verbally, it's a good idea to have the information in writing as well, so that you can supply a copy if people need it.

What exceptions apply?

There are some situations in which you will not have to inform individuals of the rule 3 matters. These situations are outlined below. In each case, you need to have reasonable grounds for why you believe the exception applies.

Exception to rule 3	Note on when the exception applies
Not complying with rule 3 is necessary to avoid prejudice to maintaining the law (including in relation to court proceedings), enforce specific laws, or protect public revenue.	This exception might apply where a public sector agency is collecting biometric information from an individual as part of an investigation of a possible offence, and informing the individual could prejudice the success of the investigation.

Exception to rule 3	Note on when the exception applies
If informing the person would prejudice the purposes of the collection.	There must be a clear link between informing the individual of the rule 3 matters and how it will prejudice the purposes of collection. E.g. if you monitor a user's behavioural biometrics as an anti-fraud measure and it appears that a possible unauthorised user is accessing the account, you wouldn't have to notify the unauthorised user. As with all exceptions, if you are collecting information from multiple individuals, you need to ensure that the exception applies to each individual.
If the biometric information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.	It is not enough to simply remove someone's name or someone's face from their biometric information. If you are publishing the information, you need to consider if the audience has any knowledge that could help them identify an individual. We have more guidance on what makes a personal identifiable. While it is not necessary to comply with rule 3 in these circumstances, if you are

Exception to rule 3	Note on when the exception applies
	using biometric information for statistical or research purposes, it will usually be good practice to still provide individuals with information on the rule 3 matters.

Rule 3 Example Scenarios

Use of FRT in a retail store to operate a watchlist

A store intends to use FRT to identify individuals on a watchlist to help improve staff and customer safety.

The store adds a large poster on the exterior wall of the entrance to the store. The poster informs people about the use of FRT and why it is being used. It also provides a link to the store's website where more detailed information about the use of FRT is available. The poster also tells people that they can ask staff members inside for more information, including printed handouts with the website information about FRT.

The store also plays an announcement with information about FRT over the store speaker system at intervals throughout the day.

There is also a smaller notice with the FRT information where customers pay for goods.

Staff members receive training on what to tell people who have questions about the FRT system.

Collection of voice sample by bank

A bank uses voice biometrics to verify its customers when they call the bank.

When the bank enrols customers into the voice verification system, a recorded message provides the customer with all the information outlined in rule 3 and confirms that the individual would like to use the voice verification system or an alternative (which is less secure). The customer is informed that all the information about the voice verification system can also be found on the bank's website.

On subsequent occasions, when people call the bank and choose the option to verify themselves as an existing customer, there will be a reminder about the collection of their voice biometrics to do this and reminds them where more information can be found (covering the minimum notification rule). The bank does not need to cover the full rule 3 matters because it did so when it enrolled them (even if the customer turns out to not be enrolled or is a fraudster).

Facial recognition in a gaming venue

A gaming venue will implement a facial recognition system for the purpose of helping staff enforce exclusion orders for problem gambling. If the system identifies a match with someone who has an active exclusion order, it will generate an alert for staff to manually review and determine it is the correct individual.

The venue will have signs installed on the exterior and interior entrance doors, as well as a few signs inside the venue.

The sign could say:

> FACIAL RECOGNITION OPERATING
>
> This venue operates a facial recognition system to monitor for people who are excluded from gambling at this venue. The system alerts staff if a person who has been excluded enters the gaming room so that staff can approach person and enforce the exclusion order.
>
> If your image is not a match for an excluded person, it will be deleted.
>
> Your image will not be collected if you stay in the pub area.
>
> More information is available on our website at [website address].

Rule 4: Be fair in how you collect biometric information

Rule 4 is about **how** you collect information – your manner of collection. You must collect biometric information in a way that is **lawful**, **fair** and **not unreasonably intrusive** in the circumstances.

What does "manner of collection" mean?

Your **manner of collection** is any steps that you take to collect the biometric information. For example:

- the device or technology used to obtain the information (e.g. FRT system),
- the method of recording the information (e.g. remotely via camera or recording device or directly via a sensor),
- the timing and context of collection (e.g. when offering a service), and
- how you act or represent yourself (e.g. how and what you tell people about the collection. See rule 3 for more information about notification requirements).

Collect biometric information in a lawful way

You must not breach the law or contravene regulations when obtaining or collecting biometric information.

Think about **what other laws** apply to the situation. For example, there are laws setting out expectations for how employers should conduct themselves in the employment relationship, including processes they must follow. Breaching these during an employment processes may mean personal information collected during that time is unlawfully collected.

If you break any law when collecting information, that will make the collection not lawful under the Code, and there may be other consequences under the law you broke or the Privacy Act.

Don’t collect biometric information in an unfair or unreasonably intrusive way

What is fair and not unreasonably intrusive will depend on the specific circumstances and context in which you are collecting the information. Take steps to ensure that people have as much control and agency over the collection and use of their information as possible, especially if there may be adverse consequences for them.

Relevant factors include:

- The **age and capacity** of the individual whose biometric information you are collecting.
    - For example, particular care needs to be taken when collecting biometric information from children and young people. It may not be fair to collect information from children in the same manner as you would from an adult. You may need to take special care with the information of young people to address any power imbalance, and to obtain their genuine consent for the collection (or consent from their family/whānau, if appropriate).
    - You should also consider other factors which may make an individual vulnerable, such as health conditions or disabilities.
- The **purpose of collection** and the **consequences for the individual** stemming from the collection and the use of their information.
    - For instance, if there are likely to be adverse consequences for the individual, this affects what would be a fair way to collect the information e.g. ensure they were notified, can opt-out of the processing or have time to address any issues with the processing.
- **What the individual has been told** about all aspects of the collection.
    - For example, was the individual informed about the collection under rule 3? Do you think they are aware about the collection? Are you collecting their biometric information from another source? Covert collection of biometric information runs a serious risk of being unfair.

- The **type and amount of information** collected.
    - For example, if your facial recognition camera captures people that you don't want or need to identify.
- **When and where** the biometric information is collected.
    - For example, are you using covert surveillance without reasonable justification? What does the individual need to do for the information to be collected? Is there a less intrusive means to collect the same information?
    - It may not be fair to collect the information in one particular context and intend to use it in a completely different context.
- Your **relationship** with and **conduct** toward the individual.
    - Threatening, coercive or misleading behaviour when collecting information is likely to make the collection unfair or unreasonably intrusive.
- Would people **reasonably expect** that their biometric information would be collected by you in the way you intend to collect it?
    - Fairness is about handling information in ways that people would reasonably expect. If people would likely be surprised or upset by the way you collect their biometric information, this could indicate that the way you are collecting information is not fair.

Using web scraping to collect biometric information

What is web scraping?

Web scraping means using automated tools to extract information from online sources including websites and social media platforms. While it can be done manually by a human user, the term usually refers to automated processes. It typically involves a software program or bot that is designed to visit web pages, retrieve their content, and process it to collect specific data, like text or images.

Web scraping can have significant privacy impacts. It enables large amounts of biometric information like facial images or voice recordings to be indiscriminately captured from websites and used without the individual's knowledge or consent. Web

scraping also enables huge databases of biometric information to be created, which can be used for large-scale surveillance.

While the information obtained through web scraping may be publicly available online, individuals may not reasonably expect their information to be used in this way. Web scraping is a form of invisible processing: where an organisation uses web scraping to collect information, the individual will not know that their information has been collected, and they cannot easily exercise their Privacy Act rights of access to and correction of their information.

Is web scraping to obtain biometric information allowed under the Code?

Using web scraping tools to collect biometric information could be a breach of the collection rules, particularly rule 4, depending on how and what is scraped and why.

You should be cautious about using web scraping as a means of collection because in some circumstances it could breach rule 4. You should consider:

- Is the scraping targeted or indiscriminate?
- How much biometric information are you collecting?
- Does the scraping circumvent online privacy controls?
- Is the scraping tool collecting information which has been shared in a specific context? (e.g. on a chat forum with restricted membership).
- What will the scraped information be used for (e.g. to train biometric recognition or classification models/algorithms? To create watchlists?)
- Is the information being scraped sensitive or are individuals concerned vulnerable in any way?
- Did the individual make the information publicly available themselves? Or has it been shared by someone else?
- What are the intended downstream uses of the biometric information? Is it likely that there will be adverse effects on people, and if so, are these warranted?
- Are you transparent about your use of web scraping tools and which online sites they scrape data from?

Overseas example: The Australian privacy regulator found that Clearview AI breached Australians' privacy by scraping biometric information from the web and disclosing it through a facial recognition tool. They found that the covert collection of sensitive information through web scraping was unreasonably intrusive and unfair. There was a lack of transparency around the collection practice, people's data was monetised by Clearview AI for a purpose entirely outside reasonable expectations, and there was a risk of adverse impacts to people whose images were included in their database.[2] These factors contributed to the finding that the web scraping was unreasonably intrusive and unfair.

Although there are differences between the Code and Australian privacy law, this example provides helpful insight into the kind of situation when web scraping could be unfair.

Rule 4 Example Scenarios

Use of FRT in retail store to operate a watchlist

A store intends to use FRT to identify individuals on a watchlist to help improve staff and customer safety.

Applying rule 4

It would not be fair for the retail store to use techniques such as web scraping to obtain images of people from news sites who may have committed crimes and pre-emptively enrol the web-scraped images into the store's FRT watchlist. This would also likely breach other rules in the Code, such as rule 1. However, it would likely be lawful, fair

[2] https://www.oaic.gov.au/news/media-centre/clearview-ai-breached-australians-privacy

and not unreasonably intrusive to use stills from the store's CCTV system to enrol the individuals into the FRT watchlist, provided the rest of the Code was complied with when doing so.

The retail store would also need to consider where the cameras were physically located. For example, if there was a camera at the entrance of the store, it would be important to ensure the camera did not capture unnecessary images of people (e.g. people walking nearby but not entering the store). Similarly, if the store had changing rooms, bathrooms or any other sensitive area, it would be important to ensure no sensitive images were being captured.

Attention monitoring in employment context for safety

A long-distance trucking business is considering implementing a biometric-based fatigue and attention monitoring system for its drivers to ensure driver safety.

Applying rule 4

The business recognises that continuous monitoring of employees while they are working is highly invasive. To comply with rule 4, they decide on a policy that presents the minimal level of invasiveness, such as setting the system to only record video not audio and turning the system off when the vehicle is not on. Video footage will only be reviewed by the employer if the driver has been involved in an incident and the driver is provided with a copy of all data the system sends to the employer.

Rule 10 would also be particularly relevant to this scenario.

Rule 5: Security of Biometric Information

Rule 5 is about protecting biometric information. You need to ensure that you protect the biometric information that you hold with security safeguards that are reasonable for the sensitivity of biometric information. The biometric information must be protected against loss, misuse, and any unauthorised access, use, modification or disclosure.

Note: Security considerations may be relevant to your use of biometrics in two ways:

1. You have an obligation to protect biometric information you hold under rule 5 in the Code.
2. You may also use biometrics as a security measure itself, as a way of meeting your obligations under IPP5 to protect other personal information, including using biometric verification or identification systems to restrict access to devices or spaces.

These two obligations are connected – protecting the biometric information you hold from misuse will help it be an effective security protection for other personal information.

Security obligations when using third party providers

If you are using a third-party service provider, then you still have the responsibility of ensuring the security of the information. You will need to do everything reasonably within your power to prevent unauthorised use or disclosure of the biometric information by making sure that the provider has their own security safeguards in place.

Other relevant guidance about security safeguards

- IPP 5 guidance. Note that rule 5 essentially replicates IPP5.
- Security safeguards in our rule 1 guidance.
- Security and Access controls in Poupou Matatapu, our guidance on doing privacy well.
- Working with third parties guidance.
- New Zealand Information Security Manual (NZISM).
- The NZ National Cyber Security Centre's Critical Controls.

International guidance on biometrics and security

- National Cyber Security Centre (UK) guidance on biometric recognition systems.
- ISO/IEC 24745:2022 Biometric information protection.

What are reasonable security safeguards?

You need to consider what is appropriate for the specific biometric information that you hold. Te ao Māori perspectives, such as protecting the tapu, mana and mauri of the data, can also inform what is reasonable for your circumstances.

Your security safeguards need to reflect the sensitivity of biometric information and the overall context and risk of the biometric information that you hold. The more sensitive the information, the more robust the safeguards need to be to limit the risk of the information being compromised. A safeguard can still be reasonable to implement even if it is difficult, expensive or takes time to implement. You need to factor in the costs of relevant safeguards to your overall planning. But, a wholly disproportionate cost or difficulty to implement could make a security safeguard no longer reasonable to implement.

The more severe the consequences for individuals from loss, misuse or unauthorised access to their biometric information, then the more likely it is that a security safeguard will be appropriate, even at a high cost or difficulty to implement.

Security safeguards must be **layered**, meaning you have multiple safeguards in place at the same time. No safeguard is complete on its own, and layering safeguards will limit the impact of one safeguard failing or being breached.

In general, you need to consider:

- How will you **protect** the biometric information within your system? Protecting information means protecting it from loss and unauthorised modifications. Protecting information includes technical controls (e.g. encryption), physical controls (e.g. locked rooms) and organisational controls (e.g. policies governing how biometric information is stored – such as storing biometric information locally if appropriate).
- How will you ensure **devices and software are kept up to date** by applying the latest updates and patches?

- Where and how is information **stored**? Will the biometric information be **kept separate from** (e.g. not linked or connected to) **other information** in your system? If it is necessary to link it to other information, what other protections can be put in place? Do you need to store the information on a central system, or can you store it across local devices i.e. on-device verification?
- What is your plan for information **back ups?**
- How will you **restrict access** to biometric information? How will you ensure only authorised people have access? (e.g. individual user logins and regular and random audits). Who is responsible for controlling access? How will you limit and identify employee browsing?
- How will you **restrict the use and disclosure** of biometric information? Can you build in technical restrictions as well as having organisational policies about the use and disclosure? Who is responsible for making these decisions?
- How will you assess whether your **safeguards are operating effectively**? What is your **vulnerability management** process?
- How are you **minimising data collected, stored and retained**? The less information you hold, the less information you have to protect. If you do not need to retain biometric information, you should delete it – for example, if you only need to retain biometric templates and not samples, you should delete the biometric samples as soon as they are processed into templates.
- How will you **safely dispose** of biometric information when it is no longer needed for your lawful purpose? Are your disposal methods appropriate for the type of information concerned? When will you dispose of biometric information?
- What **staff training** will be in place for staff involved in your biometric system?
- What is your organisation's **capability** in this area? While the size and resources of your organisation is a factor in what is reasonable, you must still ensure you have enough capability to securely deploy and manage a biometric system. This is an important consideration as off-the-shelf biometric systems become more widely available.

- If you are using a **third-party provider** to hold biometric information on your behalf, what are your rights and ability to monitor and audit that provider's security practices? What are your residual responsibilities? See our guidance on working with third parties for more information. Remember that if the third-party provider is holding the information on your behalf and not using the information for their own purposes, you are still responsible under the Privacy Act.
- What is your plan for **if something goes wrong**? Security breaches can lead to privacy breaches, but even a security breach that does not directly cause a privacy breach could weaken the biometric system and needs to be promptly addressed. Remember that if you have a **privacy breach** that either has caused or is likely to cause anyone serious harm, you must notify the Privacy Commissioner and any affected people as soon as you are practically able. See our privacy breach guidance for more information.
- Does the biometric data involve content **sensitive for Māori** e.g. moko kanohi or moko kauae and how will you address it? What mitigations are available to you to avoid breaches relevant tikanga? Have you consulted experts if appropriate?
- Can you meet **technical guidance** from relevant international bodies or experts? E.g. can you meet relevant **ISO/IEC standards** for protecting biometric information?

You should consider engaging a subject matter expert to review your planned security controls, both at the outset and at regular intervals.

Using biometric information as one of your security safeguards

Sometimes you may want to use biometric information to protect other information – for example, using biometric information as part of multi-factor authentication (MFA) to protect other information. That is, you may be using biometric information **as part of your security safeguards**. If you are doing so, you still need to ensure you are protecting the biometric information appropriately, for example by taking steps to protect the biometric information and the wider system from presentation attacks.

You need to carefully design your biometric system for your context. Different kinds of biometric systems have different strengths and weaknesses, and addressing these relative strengths/weaknesses needs to be a core part of designing the safeguards for your system. For example, a facial recognition system may have more accuracy issues in an environment with poor lighting, and so the design of the system would need to take that into account.

You will need a plan for **responding to any errors** in the system (e.g. false positive or false negatives). How will you mitigate any impacts on individuals (e.g. not being able to access a space or use a device)?

Rule 5 Example Scenarios

Facial recognition by a retail store to operate a watchlist

A store intends to use FRT to identify individuals on a watchlist to help improve staff and customer safety.

As part of complying with rule 5, the store makes deliberate decisions about how the system will operate and how the information will be protected, to help minimise the amount of biometric information collected and ensure it is adequately protected. For example:

- Immediate deletion of non-match images.
- Ensuring stored biometric information is encrypted.
- Restricting user access to the biometric system to a limited number of staff with additional training. Access is logged and there will be regular audits.
- Choosing a biometric system that complies with relevant ISO/IEC biometric standards. The system chosen also has a high level of accuracy when capturing images in the “wild” i.e. under the conditions in the store.
- Ensuring biometric templates are irreversible, unlinkable, and revocable.
- Regularly reviewing security practices and taking action on any identified issues.
- Mitigating technological issues of bias or accuracy.

- Not linking biometric information to any other customer data e.g. loyalty programme.
- Alerts from the watchlist only go to authorised devices on the store's network.
- Securely destroying biometric information when no longer needed.

Fingerprint scan for Multi Factor Authentication (MFA)

A business has access to highly sensitive information. It wants to ensure only the correct staff members have access to a limited, highly restricted database. It decides to implement a multi-factor authentication system using employee fingerprints. The business implements a range of security measures to comply with rule 5, for example:

- Processing biometric samples into biometric templates and deleting the original samples.
- Storing the biometric template locally on each employee's device and not linking the biometric template with any other employee personal information.
- Ensuring a high standard of technical protection for the biometric information.
- Keeping the employee devices' operating system and software up to date by applying latest updates and patches.
- Ensuring the business can and will audit any access (or attempted access) to biometric information.
- Securely deleting biometric information when the relevant employee no longer needs access to the restricted database.
- Regularly reviewing security practices and taking action on any identified issues.
- Having clear organisational policies and practices around how biometric information is collected, held, disclosed and destroyed.

Rule 6: Access to biometric information

Rule 6 is about an individual's right to access their information. In general, an individual has the right to receive on request:

- Confirmation of whether you hold any biometric information about them.

- Confirmation of what type of biometric information you hold about them.
- Access to the biometric information you hold about them.

If you give an individual access to their biometric information, you must also tell them that they have a right to request that their biometric information be corrected (see rule 7).

Part 4 of the Privacy Act outlines the process for handling access requests

Rule 6 is subject to Part 4 of the Privacy Act, which explains the process for requesting access, the process for charging for access, and outlines the exceptions for when you may refuse access to personal information. OPC has general guidance on access requests and the grounds that allow agencies to refuse access to personal information. The same grounds also apply to the biometrics Code.

What if an individual requests other personal information?

An individual may request other personal information in addition to their biometric information from you. For example, they might want access to both biometric information and results (outputs) from the biometric process, such as confirmation of a match (output of a verification process) or an age range estimate (output from age estimation).

Although results are not biometric information, they are still personal information about the individual and depending on the context might be sensitive information. Individuals are entitled to ask for this information under IPP6 of the Privacy Act rather than rule 6 of the Code. The process for responding to both requests is the same and in most cases you will be able to provide them to the individual at the same time.

Organisations must give reasonable assistance to anyone requesting access to their information (section 42 of the Privacy Act). If you don't know what information the individual is seeking, ask the individual to clarify. If an individual asks for the information to be provided in a specific way, you should give it to them in that way unless there is a good reason not to. These reasons are listed at section 56 of the Privacy Act.

Confirm the type of biometric information

If an individual requests access to their biometric information, unless a ground for refusing access applies, you must also confirm the **type** of biometric information you hold about them. For example, you must confirm if you hold a biometric sample (e.g. a facial image or fingerprint scan) or a biometric template or model (e.g. numerical representation of their facial features or fingerprint ridges).

An individual only needs to request access to their biometric information for the obligation to confirm the type of biometric information held to apply. The individual does not need to specifically request access to the type of biometric information separately.

The requirement to confirm the type of biometric information you hold is in the Code to support people's privacy rights in a context where it may be difficult to provide someone with meaningful or actual access to their biometric information. Biometric information may not be readable or understandable by people, or even by other biometric systems. It may also not be possible to extract the biometric information and provide the individual with their biometric information in hard copy or a common electronic form (see below for more information about when the information is not readily retrievable).

When you confirm what types of biometric information you hold, consider also providing a description of the information to help the individual understand what biometric information you hold about them and, if relevant, why you cannot provide a copy of the information. Although providing a description is not required by the Code, it may be frustrating for individuals to not be able to receive access to their biometric information in a meaningful way. Providing information about the form of information you hold and how it's used in the system may be helpful to individuals. Remember that individuals are entitled to complain to OPC about an organisation's failure to provide them with access to their information.

Providing access to biometric information

Providing someone with access to the biometric information you hold about them could mean:

- You send a copy of a biometric sample you hold, for example, a copy of a fingerprint or a copy of a photo of their face.
- You allow the individual to view their biometric sample on your premises.
- You provide the individual with a copy of their biometric template. If you do this, consider also providing an explanation of what it is (as it otherwise may not be readily understandable by the user).
- You provide the individual with a copy of a biometric sample, and you also inform them that you hold a biometric template related to that individual. This could apply if it is not possible to extract a biometric template (or other biometric information) from your biometric system.

Grounds for refusing to provide access to biometric information

OPC has guidance on when you can refuse access requests that explains the permitted grounds for refusing access to personal information in the Privacy Act that also apply to providing access to biometric information.

Readily retrievable information

You need to provide access to readily retrievable biometric information. OPC's general guidance on what is considered readily retrievable information will apply to biometrics too.

If the biometric information cannot be easily isolated or extracted from the biometric system, then the information will not be considered readily retrievable. But, when you are designing a new biometric system, being able to respond efficiently to an access request should be part of the system design.

Information about more than one person

Another ground for refusing access to biometric information could be if the information contains information about more than one individual – e.g. if you hold a similarity score

comparing two faces or a list of potential matches generated in an identification process.

If the information is about more than one person, you need to consider whether providing access to the requestor would be an unwarranted disclosure of the affairs of another person. We have guidance on responding to requests for access for information about more than one person.

You don't need to keep biometric samples for responding to access requests

An important security measure for biometric information can be deleting original biometric samples once they have been processed into a biometric template. If it is appropriate in your overall circumstances to delete biometric samples, you can do so, and this is not a breach of rule 6 (and it may even be part of complying with rule 9).

Rule 6 Example Scenarios

Facial recognition by a retail store to operate a watchlist

Topics covered: confirmation of type and access to biometric sample

A store uses FRT to identify individuals on a watchlist of previously violent customers to help improve staff and customer safety.

The store receives a request from two individuals for access to their biometric information:

- The store confirms that the first individual is not on the watchlist. Then, because non-match images are immediately deleted, the store searches and informs the first individual that it does not hold any of their biometric information.
- The store confirms that the second individual **is** on the watchlist. It holds a biometric sample (a face image from CCTV still) that was used to enrol the individual on the watchlist. The sample was retained so that the trained staff members can refer to the image to confirm whether a possible match generated

by the biometric system is accurate. The store also holds a biometric template of that individual's face. The store informs the individual that it holds both a biometric sample and a biometric template of their face. It provides the individual with a copy of the CCTV still. The face template cannot be extracted from the system, so the store provides confirmation that it does hold a template related to the individual used to identify if they walk in the store but it is not readily retrievable.

Fingerprint scan for Multi Factor Authentication (MFA)

Topics covered: access to biometric template

A business is using a multi factor authentication (MFA) system using employee fingerprints as one authentication factor. An employee makes a request for their biometric information. The employer holds a template of the fingerprint that the system uses to verify the employee's identity. It is possible to extract the fingerprint template from the system, but it is not something that would be readily understandable (because it looks like a random sequence of numbers).

The employer provides the employee with a copy of the fingerprint template, even though the template is not understandable outside of the context of the system. They also decide to provide a brief written explanation of what the template means and how it is used by the fingerprint recognition system to verify the employee.

Rule 7: Correction of biometric information

Rule 7 provides that a person has a right to ask you to correct information about them if they think it is wrong. Upon this request, or on your own initiative, you must take steps to ensure that the information is accurate, up to date and complete and not misleading for the purpose you are using it for.

Failing to respond to a correction request could also breach the rule 8 requirement to take steps to ensure the accuracy of the information you hold.

Part 4 of the Privacy Act outlines the process for handling correction requests

The rules for how an organisation must respond to a correction request are set out in Part 4, Subpart 2 of the Privacy Act 2020. OPC has general guidance on correction requests that could help you to respond.

What if an individual asks us to correct other personal information?

An individual may ask you to correct other personal information in addition to their biometric information that you hold. For example, they might want you to correct both their biometric information and results (outputs) from an identification or verification process. The process for responding to requests under the Privacy Act and the Code is the same and you can do both at the same time.

If you don't know what information the individual is seeking to correct you should ask the individual to clarify.

What if you don't agree with the correction request?

If you do not agree that the information needs correcting, for example, because you have taken reasonable steps to ensure the information is accurate and you believe it is accurate, the individual can ask you to attach a statement of correction to their records, and you must take reasonable steps to do so. You also need to take reasonable steps to ensure the statement of correction will always be read alongside the person's information.

If you correct the individual's biometric information (or attach a statement of correction to it), as far as reasonably practical, you must also inform every other person to whom you disclosed that biometric information to (note also that any disclosure of biometric information needs to comply with rule 11 and rule 12).

What correcting biometric information could look like

If you receive a request to correct a person's biometric information, you must take reasonable steps to satisfy yourself about whether the information you hold is correct. See also the rule 8 accuracy requirements.

Depending on the individual's information and reason for requesting a correction, you could correct someone's biometric information by:

- Completely removing the individual's information from your system and re-enrolling them with new information e.g. a new image or other biometric sample. If you do this, consider whether it is appropriate to keep a record of the fact that you have removed/replaced the person's information. In general, you don't need to retain a copy of the original information that you removed (unless other legal requirements apply).
- Removing or deleting someone's biometric information entirely from the system if they have been incorrectly enrolled, misidentified, or have asked to be deleted.
- Adding a person's statement of correction alongside their biometric information within your system so it always read alongside that information (this may be the right step where you are confident the information is accurate and have taken reasonable steps to verify the accuracy of the information, but the individual disagrees).
- Regenerating a biometric template based on an existing biometric sample (this could be appropriate if there have been updates to the biometric system).

Rule 7 Example Scenarios

Facial recognition to control access to restricted site

A company is using FRT to control access to a restricted site. A staff member who should have access to the restricted site is repeatedly rejected by the FRT system. The staff member believes their biometric information needs to be corrected to resolve the issue. The company investigates and determines that the original biometric sample (photo of staff member) was not high enough quality to give consistent accurate results.

The company responds to the request by completely deleting the staff member's existing biometric information. They then generate a new biometric template from a new biometric sample (photo of the individual).

Facial recognition by a retail store to operate a watchlist

A store uses FRT to identify individuals on a watchlist of previously violent customers to help improve staff and customer safety. An individual was flagged as being on the watchlist and asked to leave the store. The individual requests that the store corrects their biometric information by deleting their information from the watchlist (correction requests can include asking that information be deleted). How the store corrects the information could change depending on whether and why correction is needed:

- If the individual should not be on the watchlist at all (e.g. because the store accidentally enrolled the wrong person onto the watchlist), the store would need to completely remove the individual's biometric information from the watchlist.
- If the individual was not on the watchlist, but was misidentified due to a false positive (incorrect match), the store would need to assess whether to:
    - Add a note in the system about past false positives/incorrect matches that would appear if the system identifies the person who is enrolled on the watchlist, in order for a staff member doing a manual review to have more context. This could also be appropriate for situations like if an individual has a twin or sibling who looks very similar.
    - Regenerate a biometric template for the person who is meant to be on the watchlist using a better-quality sample (e.g. CCTV still), if the enrolled photo is poor quality and contributed to the misidentification. Doing this would also help comply with the accuracy requirements in rule 8.

Receiving a correction request because of misidentification is a good prompt for the store to consider other changes to ensure the overall accuracy of the system and meet their obligations under rule 8. Some of the changes that the store should consider are:

- Reviewing the system's match threshold settings if the sensitivity setting is set too low and so the system is producing incorrect matches at too high a rate.
- Removing the relevant biometric information for the correct person on the watchlist if the enrolled photo is not of sufficient quality to avoid further misidentifications for the person requesting correction.
- Changing the process for responding to alerts to reduce the risk of subsequent misidentifications, for example by strengthening the manual staff review process (see also our rule 1, rule 5 and rule 8 guidance).

Rule 8: Accuracy of biometric information

Rule 8 says that you need to take reasonable steps to make sure any biometric information you hold is accurate, up to date, complete, relevant and not misleading, before you use or disclose it. Part of this requirement is ensuring that your overall biometric system is sufficiently accurate for your purpose and the overall risk and context.

We have general guidance on ensuring the accuracy of personal information that also applies to biometric information.

How can you ensure that the biometric information you hold and the operation of your biometric system is accurate?

What is reasonable in the circumstances to avoid accuracy errors will change depending on your overall risk profile (the type of information you hold, what it is being used for, your context, and the potential harm that individuals may experience).

Example steps to ensure accuracy:

- Ensure the biometric system is using sufficiently high-quality samples e.g. photos, audio recordings.
- Keep biometric samples up to date as required and generate new biometric templates when needed (for example, due to aging, surgery or injury).

- Where necessary, implement manual (human) review of matches by the biometric system before taking action based on the biometric system. You also need to ensure the staff involved have appropriate training and are effectively equipped to challenge the accuracy of results if needed. This is sometimes called having a “human in the loop”. Having a human in the loop will be essential for some uses of biometric information – for example, if you are operating a biometric watchlist or any other context where people could be negatively impacted by the use of their biometric information.
- Regularly review and refine the sensitivity and specificity settings of the biometric system to ensure the rate of any false positive or false negative matches is appropriate for the use case and not leading to adverse outcomes for individuals.
- Select a biometric system with appropriate accuracy for your privacy risk and overall context. Some systems show better performance in certain contexts or for certain uses than others, especially in different conditions (i.e. in the wild versus controlled environments). You should refer to independent evaluations (e.g. by NIST) of the accuracy where possible.
- Train staff and any other users of the biometric system about what a match means, so that they better understand the results of a biometric system and can respond appropriately. For example, a match resulting from a verification process is not a definitive determination of a person’s identity – it reflects the statistical likelihood that this person is same as the identity they are claiming.
- Have a process or audits in place to identify and resolve errors and issues related to the biometric system, including understanding and mitigating any bias in the system (such as the system being less accurate for a particular demographic group or skin tone). The risk of inaccuracy from bias needs to be addressed both with human review (e.g. training, two person check before acting on an alert) and system checks. Unaddressed risk of bias may compromise the accuracy of the system.

- Ensure individuals can raise concerns about the accuracy of the system and you have a process in place to respond (see also our guidance on rule 7 – correction of biometric information).
- Testing the system before you officially deploy it e.g. on training data that is representative of the people whose information you will process.
- Conduct due diligence when choosing or procuring a biometric system or service provider, and consider the suitability for the setting the system will be used in and the New Zealand demographic.

Does the biometric system need to have 100% statistical accuracy?

No. Biometric systems, by nature, are probabilistic which means they assess likelihoods not absolutes. So, there's no such thing as 100% accuracy; a biometric system will always have some margin of error.

However, to comply with rule 8, your biometric system does need to be sufficiently accurate for the overall context, privacy risk and people whose information you are collecting. In most cases, this means your system needs to be accurate in the vast majority of cases (i.e. highly accurate). If you operate a system that is not very accurate, it will be hard to show that it is necessary and effective (therefore, you may be in breach of rule 1). You also need to have a process in place to effectively mitigate the risk of misidentifications, so that the system as a whole is highly accurate.

You should consider how inaccuracies (misidentifications or mis-categorisations) could impact individuals – for example, by causing embarrassment or impacting on a person's dignity and feelings. For Māori individuals, inaccuracies may also undermine the tapu, mana and mauri associated with Māori biometric information, so you should have a culturally responsive plan to address inaccuracies.

You also need to have processes in place to mitigate the harm from any incorrect identification, verification, categorisation or inference.

The statistical accuracy of your biometric system is also relevant to other rules. For example, rule 1 (your system must be necessary, effective and proportionate with relevant safeguards in place) and rule 4 (making sure your means of collection is fair).

Rule 8 Example Scenarios

Facial recognition by a retail store to operate a watchlist

A store uses FRT to identify individuals on a watchlist of previously violent customers to help improve staff and customer safety. When selecting the FRT provider, the store investigated several different systems with varying performance metrics, including different accuracy rates.

The store chooses to contract with a FRT provider of a system with a high level of accuracy. Given the significant impact on individuals and the store from any potential misidentifications (false positives and false negatives), it is reasonable in the circumstances for the store to choose a system that is highly accurate and reliable, compared to other options.

The quality of the enrolment biometric samples is also important. The store only enrols individuals on to the watchlist if it has a sufficiently high-quality image from CCTV or another appropriate source. Using lower quality samples increases the risk and rate of misidentifications and may mean the system is not sufficiently accurate to comply with rule 8.

Facial recognition to control access to restricted site

A company is using FRT to control access to a restricted site. A staff member who should have access to the restricted site is falsely rejected (a false negative) by the FRT system. This single misidentification, in itself, wouldn't necessarily be a breach of rule 8, provided the company had a process in place for the staff member to challenge the misidentification, the misidentification was not a systemic issue, and the company had a process in place to regularly review any misidentifications and revise the match sensitivity settings as appropriate.

Rule 9: Retention of biometric information

Rule 9 is about how long you can hold (keep) information for. You must not hold biometric information for longer than is required for the purpose you are using the information for.

Limiting how much information you hold and how long you hold it for is a key way that you can lower the privacy risk of your processing – for example, immediately deleting biometric information that does not return a match in a FRT system means you will hold much less biometric information overall and effectively reduce privacy risks like over-collection, surveillance, scope creep, and security breaches.

Reminder: under rule 3, you must notify individuals about your retention policy for biometric information. This could include a timeframe or summary of your policy that tells individuals how long you intend to retain their information for.

How long can I retain biometric information?

In most cases, if you do not have an active and lawful reason to **use** the biometric information, it will no longer be appropriate to hold it.

You also need to consider what you told the relevant individual when you first collected the biometric information.

For Māori biometric information, consideration should be given to the tapu and mana of the owner over their biometric information in regard to retention given its potential cultural significance.

What about other legal requirements?

There are some laws that may allow or require an organisation to retain or delete biometric information in certain situations or in a certain way. For example:

- Section 288 (3) of the Immigration Act 2009
- Section 85 of the Policing Act 2008

- Public Records Act. Public sector agencies can find guidance on the Public Records Act at Manage information – Archives New Zealand (external link).

How to manage retention as an organisation

We recommend setting-up retention and disposal systems. These may look like:

- Automated deletion: If possible, set up your systems to action your retention and disposal decisions in an automated way. Not doing so is a common cause of over-retention issues in organisations.
- Manual deletion: If there is no ability to automatically dispose of biometric information. You will need to consider other ways, such as regular audits or manual review of the biometric information you hold.
- Different retention periods for different information: You also need to ensure that retention periods can be tailored for different circumstances. For example, if you are collecting different types of biometric information for different uses, some biometric information may need to be disposed of sooner than others.
- Have a clear process outlined in a policy: Your organisation should have a clear process to support the lawful retention and disposal of biometric information.
- Regular review: Retention and disposal policies should be regularly reviewed to ensure that they are fit for purpose and being appropriately followed in practice.
- Effective disposal: you need to consider how to effectively dispose of biometric information so that it is irretrievable.

Rule 9 Example Scenarios

Collection of voice biometrics by bank

A bank uses a voice verification system as part of their identity verification process when customers call the bank, to detect and prevent fraud.

The bank assesses how long to retain the voice-based biometric information it collects and decides:

- It will retain the original voice sample used to enrol each customer and store it securely.
- The bank establishes a policy governing how long subsequent voice samples (e.g. probe recordings) for each customer will be kept for that is based on advice from the bank's security experts and the bank's legal obligations. The bank considered deleting these subsequent samples, but determined that its purpose will be better achieved by retaining the sample to allow for manual review if there is any suspected fraudulent activity on a customer's account and to improve the template for each individual. Therefore, keeping a larger number of samples is justified in this case.
- If a customer switches to another bank, closes their account, or passes away, the bank will dispose of the customer's voice recordings and templates within one month of account closure (unless another law requires that they be kept for longer).

Fingerprint scan for Multi Factor Authentication (MFA)

An organisation has highly sensitive information that a limited number of employees have access to. They use a biometric authentication factor (fingerprint) as part of their multi factor authentication (MFA) system to protect and facilitate access to the database.

The organisation disposes of the fingerprint scan once it has been processed and only retains the fingerprint template. Retaining the original fingerprint scan is not necessary for the system to run, so the employer does not have a legal purpose to retain it.

The organisation implements a disposal policy that covers staff who leave employment or change role within the organisation. For instance, the employer builds the removal of biometric information from their systems into the offboarding process. The employer runs regular audits to ensure that the automated disposal decisions are functioning as intended.

Facial recognition to control access to restricted site

A company is using FRT to control access to a restricted site.

The business decides to retain the original face images of authorised workers so that the supervisor can compare the images of authorised workers with the live camera footage of the person that triggered the alert (human review).

Images of workers that generate positive matches (meaning they are authorised to enter site) will be deleted immediately. Images from negative matches (possibly unauthorised workers attempting to enter site) will be retained until a supervisor confirms whether access should be granted or not, after which they will be deleted.

When an authorised worker no longer requires access to the restricted area, their face image and associated face template will be deleted. This information is deleted because the business no longer has a lawful reason to retain this information and also to ensure that previously authorised workers do not continue to have access when they shouldn't.

All biometric information (face images and templates) will also be deleted if the restricted area no longer needs to be restricted.

Rule 10: Limits on use of biometric information

Rule 10 is about what you can use biometric information for.

The general rule is that you can **only use biometric information for the purpose you collected it for**. In addition, you may not use biometric information for **biometric categorisation** unless an exception applies.

Use only for the purpose you collected it…

Rule 10 provides that you can generally only use someone's biometric information you hold for the specific purpose you collected it.

…unless an exception applies

If one of the following exceptions apply, you may use an individual's biometric information for a different purpose than the one you collected it for.

You may use biometric information for a different purpose if:

- The new purpose is directly related to the original purpose for which you collected the information.
- The way the information will be used will not identify the individual.
- The information will be used for statistical, or research purposes and it won't be published in a way that could identify the individual.
- The individual authorises the use of their information for the new purpose.
- The source of the information is a publicly available publication and, in the circumstances of the case, it would not be unfair or unreasonable to use the information.
- Using the information for the new purpose is necessary:
    - To avoid prejudice to the maintenance of the law by a public sector agency or to enforce a law that imposes a monetary penalty.
    - To protect public revenue.
    - For court or tribunal proceedings.

Note: the "avoid prejudice to the maintenance of the law" exception would not generally permit a retailer to use their biometric system to identify any person who may be wanted by a law enforcement agency. But it could apply as a one-off incident in relation to a specific investigation by a law enforcement agency.

- Using the information for the new purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual.

You need to have reasonable grounds to believe that the exception applies. Exceptions should only be used after confirming that it applies to each use of biometric information.

More information about the exceptions listed above is included in our rule 2 guidance.

The rule 10 exceptions **do not apply to biometric categorisation**. This means that even if one of the exceptions to the general limits allows you to use the biometric information for another purpose, that other purpose is still subject to the limits on biometric categorisation. The necessity and proportionality use limits also still apply if you are starting biometric processing on information you collected for a purpose other than biometric processing, or if you are changing the type of biometric processing.

Limits on biometric categorisation

Rule 10 contains limits on using someone's biometric information to categorise them or infer (or attempt to categorise or infer) certain sensitive information about them unless an exception applies (also referred to as biometric categorisation or inferential biometrics).

The Code limits certain uses of biometrics to make inferences or categorise people because inferring some types of sensitive information from the way someone looks, moves or behaves can be deeply invasive of an individual's privacy, whether or not the categorisation or inference is accurate.

What is biometric categorisation?

Biometric categorisation (sometimes called inferential biometrics) is when an organisation uses an automated process to analyse a person's biometric information to collect, infer or detect certain other types of sensitive information about them (e.g. information about their health or information about their mood or alertness) or to place them in a demographic category (e.g. age, gender or ethnicity categories).

Biometric categorisation doesn't include:

- when a system analyses a person's body or appearance to detect a readily apparent expression (e.g. whether someone is raising their hand), or

- any process that is part of another service or device that analyses the user's biometric information solely for the purposes of providing the user with their own information or entertainment (e.g. a consumer smartwatch that provides the wearer with information about their energy levels).

Read more about the definition of biometric categorisation here.

What are the limits on biometric categorisation?

The Code places limits on using biometric information for biometric categorisation. Unless an exception applies, you must not process someone's biometric information:

- to obtain, infer or generate information about their:
  - **health**
  - **emotion**, mood, personality, mental state or intention
  - **attention** level, state of fatigue or alertness
- to **categorise** them according to categories that are **protected grounds** in the Human Rights Act.

See below for more guidance on each of the limits and relevant exceptions below.

Limit on biometric categorisation – detecting someone's health information

You must not use a biometric system to analyse someone's biometric information to obtain, infer or detect their health information unless an exception applies.

For example, unless an exception applies:

- You cannot use gait analysis to infer or detect whether an individual has a medical condition that affects movement.
- You cannot detect skin conditions to provide targeted advertising for skin care products.

You are permitted to use biometric categorisation to detect or generate health information if one of the following exceptions applies:

- You have obtained their consent (express authorisation).
- The information is necessary to assist an individual with accessibility.
- The information is necessary to prevent or lessen a threat to the life or health of an individual or public safety.
- The information is going to be used for statistical or research purposes, has ethical oversight and approval, and won't be published in an identifiable form.

The limit also won't apply if:

- You are health agency providing health services to that person.

What is health information?

Health information is defined in the Health Information Privacy Code. Health information is information about a person's health and includes information about their medical history, any disabilities they may have or have had, and information about health services that individual may have or have had in the past.

Limit does not apply if you are a health agency providing health services

As outlined above, the limit on using biometric categorisation to collect or detect health information does not apply to health agencies. This is because the Code does not apply to health agencies that are collecting biometric information to provide health services, so they are not subject to the limits in rule 10 (or any part of the rest of the Code, instead the HIPC applies to their use of information).

Limit does not apply if individual has given their consent

If you have obtained the individual's express authorisation to do so, you are not restricted from using biometrics to detect information about that person's health.

Express authorisation means that you have met the following conditions:

- Informed the individual of all relevant information about the collection and use of their information,

- given a genuine choice to the individual about whether to authorise the biometric categorisation, and
- not pressured or coerced the individual into authorising the use of their information.

Example of when the authorisation exception **may** apply:

- You give the individual all the relevant information and they expressly authorise you to infer or detect their health information through biometric categorisation e.g. to analyse their skin to detect a skin condition.

Example of when the authorisation exception **would not** apply:

- You are relying on implied authorisation, rather than express authorisation.
- You did not adequately inform the individual about all the important information in advance (see rule 3 for more information on notice requirements).

Limit on biometric categorisation – monitoring attention, fatigue or alertness

You must not use a biometric system to infer or monitor someone's state of fatigue, alertness or attention level unless the exception for health and safety, or another exception, applies.

For example, unless an exception applies:

- You cannot use biometric information to monitor what someone is paying attention to.
- You cannot use biometric information to detect whether someone is feeling fatigued (tired).

Exception for health and safety purposes

You may use biometric categorisation to infer or detect information about an individual's state of fatigue, alertness or attention level, if you believe on reasonable grounds that

doing so is **necessary to prevent or lessen a risk to public health, public safety or the life or health of any individual**.

Exception **may** apply:

- You are an employer with employees in a potentially hazardous environment (e.g. operating heavy machinery) and you intend to use biometric categorisation to detect fatigue or loss of alertness/attention in drivers to reduce the risk of a crash or other accident.

Exception **would not** apply:

- You are an employer in an office-work type environment and you want to detect alertness or attention to monitor employee productivity. Monitoring productivity is not necessary to reduce a risk to health, life or safety.

Other exceptions that could apply to monitoring attention, fatigue or alertness:

- The information is necessary to assist an individual with accessibility.
- The information is going to be used for statistical or research purposes, has ethical oversight and approval, and won't be published in an identifiable form.

Limit on biometric categorisation – inferring someone's emotions, mood, or personality

You must not use a biometric system to analyse biometric information to infer information about an individual's **emotions, mood, personality, mental state or intention**, unless an exception applies. For example, you are generally not permitted to use biometric categorisation to analyse facial features and expressions to infer someone's personality traits (such as their levels of extroversion, conscientiousness, openness, agreeableness and neuroticism).

Examples of biometric categorisation that would be restricted under this limitation:

- Analysing verbal interaction to infer the emotions of two employees.

- Inferring an applicant's personality traits from facial movements and gestures in video interview.
- Detecting whether an employee is likely to be lying from eye movements in workplace disciplinary process.
- Monitoring customer emotional reactions to products and displays in a retail store.

Exceptions to limit on inferring emotions, mood or personality

However, the limit on using a biometric system to analyse someone's biometric information and infer information about their emotions, personality or mood does not apply if:

- The information is necessary to assist an individual with accessibility.
- The information is necessary to prevent or lessen a threat to the life or health of an individual or public safety.
- The information is going to be used for statistical or research purposes, has ethical oversight and approval, and won't be published in an identifiable form.

Limit on biometric categorisation – putting people into categories based on protected grounds under the Human Rights Act

You must not use a biometric system to analyse someone's biometric information and **categorise them** into categories that correspond to the prohibited grounds of discrimination listed in section 21(1) of the Human Rights Act.

For example:

- Analysing facial features to infer someone's gender, ethnicity or disability.
- Recording information about someone's physical reaction (e.g. to political advertisements) to infer political beliefs.
- Categorising a customer by any restricted category (e.g. sexual orientation) to change what products are offered or change the price of product offerings to that customer.

The prohibited grounds of discrimination in the Human Rights Act that you may not use biometric information to categorise people according to include:

- Sex, which includes pregnancy and childbirth.
- Marital status.
- Religious or ethical belief.
- Colour, race, ethnicity, nationality or citizenship.
- Disability, which includes physical disability or impairment, physical or psychiatric illness, intellectual or psychological disability or impairment, reliance on accessibility aids like a guide dog or wheelchair and certain other factors.
- Political opinion, which includes the lack of a particular political opinion or any political opinion.
- Employment status.
- Family status.
- Sexual orientation.

For more detail, see section 21(1) of the Human Rights Act.

Categorising by age or other demographic category (that is not a prohibited ground of discrimination under the Human Rights Act)

The limit does not apply if you are categorising the relevant individual by **age** or by a demographic category that is **not** a prohibited ground of discrimination under section 21(1) of the Human Rights Act.

For example:

- You are using a system to estimate the age of a person to monitor an age-based access limit to a website.
- You are using categorisation to sort photos of individuals into age groups (children, adult, elderly).
- You are categorising individuals into demographic categories that **are not** prohibited grounds of discrimination e.g. by education level.

Other exceptions for demographic-based categorisation

The limit on using biometric categorisation to a biometric system to analyse someone's biometric information and categorise them according to a protected category does not apply if:

- The information is necessary to assist an individual with accessibility.
- The information is necessary to prevent or lessen a threat to the life or health of an individual or public safety.
- The information is going to be used for statistical or research purposes, has ethical oversight and approval, and won't be published in an identifiable form.

More information about the exceptions to the biometric categorisation limits

As outlined above, there are some limited circumstances where the limits on biometric categorisation don't apply. However, you must still comply with the other requirements in rule 10 about the purpose for which you can use information.

Exception for assisting a person with accessibility

You believe on reasonable grounds that using biometric categorisation is necessary to assist an individual with **accessibility**.

Accessibility means you are helping someone with a disability overcome or reduce barriers they face to participating on an equal basis with others.

Exception **may** apply:

- You are using biometric categorisation to generate descriptions of people and the surrounding environment to provide to people with vision impairments.

Exception **would not** apply:

- You are using biometric categorisation to detect whether an individual has a disability for your own information and not to assist with accessibility e.g. you want to provide targeted advertising.

Exception for responding to serious threats to individual or public safety

You believe on reasonable grounds that using biometric categorisation is necessary to prevent or lessen **a serious threat** to public health or public safety, or to the life or health of any individual.

Exception may apply:

- You are a law enforcement agency responding to an urgent and critical situation that requires you to locate an individual in a crowd to avoid a serious threat to public safety, and using biometric categorisation is necessary to quickly locate the individual (e.g. you know some characteristics of the individual such as their race and sex, so the biometric categorisation helps narrow the possible identity of the person).

Exception would not apply:

- There is a serious threat to life or health but using biometric categorisation (e.g. detecting emotions or categorising an individual into demographic categories) would not help mitigate or resolve the threat.

Exception for conducting statistical analysis or research

The biometric information is to be used for statistical or **research purposes subject to ethical oversight and approval** and will not be published in a form that could reasonably be expected to identify the individual concerned.

Exception **may** apply:

- You are a research group conducting a study assessing the technical accuracy of a new type of biometric categorisation for detecting emotions in non-verbal individuals, you have received ethics approval for that research, have complied with the conditions the ethics committee recommended, and you otherwise comply with all rules in the Code.

Exception **would not** apply:

- You are conducting product testing to trial a type of biometric categorisation, but you do not have ethical oversight or approval of the research.

Using previously collected information, or biometric information for a different type of processing

Rule 10 also limits organisations from starting to use personal information that wasn't originally collected for biometric processing in a biometric system (e.g. photos, video or audio footage) unless it would be necessary and proportionate, and they have put in place appropriate safeguards.

It also limits organisations using biometric information for a different type of processing than it was collected for unless the use is necessary, proportionate and relevant safeguards have been adopted. These restrictions reflect the threshold for collecting biometric information in rule 1 and ensures that the important and fundamental controls on biometric processing apply to the information an organisation already holds before it adopts new biometric processing or a different type of processing.

When do you need to assess necessity, proportionality and appropriate safeguards for processing information you already hold?

If you collected biometric information in accordance with rule 1, and you are using the biometric information for the same type of processing, then you do not need to reconsider the necessity, proportionality and safeguards under rule 10.

However, you will need to consider the necessity and proportionality of your use and the relevant safeguards if:

- You are starting new biometric processing on information you did not collect in accordance with rule 1, or
- You are using biometric information for a **different type** of processing than it was originally collected for.

For example:

- You want to use facial recognition technology on an archive of CCTV footage that was not collected for biometric processing.
- You hold a database of lawfully collected images of people that were not collected for biometric processing. You want to run a biometric deduplication process on the database to remove any duplicate images.
- You want to change from using a biometric verification system to using a identification system to control access to a secure place.

Full guidance on how to assess the necessity, proportionality and relevant safeguards is included in our rule 1 guidance.

Rule 10 example scenarios

Employer use of biometrics to monitor attentiveness and detect health information to reduce risk of harm

An employer operates a work site where employees operate heavy machinery, sometimes without other people present. To reduce an identified risk of serious harm or injury, the employer needs to install cameras and use biometrics to monitor employee focus/attentiveness and monitor for health events like a loss of consciousness or injury to the employee, so that an alert can be sent to get help and machinery automatically stopped if necessary. The biometric system that the employer is considering also offers the ability to infer emotions based on facial expressions.

In this situation:

- Monitoring attentiveness or focus would likely be permitted under the rule 10(8), the exception that permits detecting fatigue, attention and alertness if doing so is necessary to prevent or lessen a risk to life or health.
- Detecting health information, such as detecting a loss of consciousness or an injury, would likely be permitted under rule 10(9), the exception for collecting health

information if the individual authorises it. The serious threat to life or health exception (rule 10(7)(b)) could also apply, depending on the level of risk to the employee – e.g. if the employee operating the machinery had a medical condition that required additional monitoring and they were operating the machinery in a high-risk environment.

- Inferring emotions would **not** be permitted as it is restricted under rule 10(5) and no exception applies that would allow it.

Employment law obligations, including consultation with workers, should also be considered when setting up these systems because of the way they capture sensitive information about employees.

Use of biometric categorisation in a call centre

The manager of a call centre is considering using biometric categorisation as part of call centre operations:

- They want to use a biometric-based productivity monitor on the work devices that employees use. The monitor uses biometric categorisation to detect what an employee is focusing on as well as their energy levels, stress and emotional reaction to calls.
- They also want to use biometric categorisation-based analysis on incoming calls to detect the mood and reactions of callers to adjust queue positioning and allocate calls among staff members.

In this situation:

- Monitoring employee attentiveness, focus or emotions etc. would likely **not** be permitted in this type of situation. It is unlikely that using biometric categorisation in this way would be necessary to lessen a threat to safety, life or health, and no other exception would apply.

- Similarly, using biometric categorisation to detect caller emotions would also likely **not** be permitted. Again, it is unlikely that it would be necessary to lessen a threat to safety, life or health, and no other exception would apply.

A possible scenario where using biometric categorisation **could** be permitted in a call centre could be for a crisis or emergency line, where callers are more likely to be experiencing high levels of distress or in dangerous situation. In that case, using biometric categorisation to detect emotions or monitor employee fatigue etc. could be permitted if it was necessary to prevent a serious threat to life or health. However, most call centres are unlikely to meet this threshold.

Rule 11 Disclosure of Biometric information

Rule 11 is about disclosing (sharing) biometric information. You must not disclose any biometric information to any other person or organisation unless there are valid grounds for that disclosure.

If you are disclosing biometric information overseas, you also need to comply with additional requirements in rule 12.

Note that sending biometric information to a third-party to hold, store or process solely on your behalf, where that third-party will not use or disclose the biometric information for their own purposes, is not considered a "disclosure". See our guidance on working with third-parties for more information.

Sharing provisions in other legislation

Disclosing biometric information may also be permitted under other legislation. If another piece of law specifically authorises or requires you to disclose the biometric information, the rule 11 restriction on disclosure will not apply.

Other legislation may also have tighter restrictions on the disclosure of biometric information than rule 11. If another piece of law specifically restricts the disclosure of biometric information, that law takes precedence.

Exceptions: When you can disclose biometric information

You can disclose biometric information if you believe, on reasonable grounds, that one of the below exceptions applies.

What does believe on reasonable grounds mean?

All the exceptions require you to have a reasonable belief that the exception applies.

A reasonable belief requires more than just suspecting something might be the case – you must have some evidence for why you think an exception applies. You should keep a written record of why you believe the exception applies. This can be done in advance – for example, your Privacy Impact Assessment (PIA) could outline common times you will share information and which exception would apply. But you must still have a reasonable belief that a relevant exception applies, each time you disclose biometric information.

If you aren't sure whether an exception applies, you must not rely on that exception. If no exception applies, you must not disclose the biometric information. Sometimes, more than one exception may apply to your situation. You should still record the reasons for relying on each exception.

Rule 11 Exceptions

Some of the rule 11 exceptions (for example, avoiding prejudice to the maintenance of the law), are also exceptions in other rules. The same general guidance for those exceptions applies to the exception in each rule.

Exception	When the exception applies
Disclosing the information is one of the purposes that the information was obtained for, or it is directly related to that purpose.	Exception **may** apply: • You need to share the biometric information to achieve your lawful purpose (and you told people you may share their information under rule 3, unless a rule 3 exception applied)

Exception	When the exception applies
	e.g. you are collecting information to detect fraud, and if you detect fraud you will pass information on to other agencies who need to know about the fraud to investigate or take action. Exception **would not** apply: • The disclosure was not one of the purposes for collection, but you think it would be convenient or useful for you to disclose the information to another organisation.
You are disclosing the biometric information to the person whose information it is.	Exception **may** apply: • You disclose someone's biometric information directly to them e.g. you give a copy of a biometric sample, like a voice recording that was used for verification, directly to the person. Exception **would not** apply: • You provide the information to a relative of the individual and request they pass it on to the relevant individual. (But see the next exception if the individual has authorised the disclosure to their relative)
The individual authorises you to disclose the biometric information.	Exception **may** apply: • The individual has authorised you to disclose their biometric information, after you've given them all the necessary information so they understand why you want to share their biometric information and

Exception	When the exception applies
	with which people or organisations it will be shared. Exception **would not** apply: • You haven't provided all the information the individual needs – for example, you didn't explain who you will disclose the biometric information to, or why. • You are aware that someone has pressured, coerced or threatened the individual into authorising the disclosure.
The information was collected from a publicly available publication, and it is not unfair or unreasonable in the circumstances to disclose it.	Exception **may** apply: • You are disclosing biometric information you collected from a public register e.g. a public picture, and there are no specific circumstances that make it unfair to disclose it. Exception **would not** apply: • You are disclosing biometric information you collected from photos on social media that required you to have additional permission to view the photos (such as being a friend or a follower of the social media account, which would mean the information is not publicly available). • The information was collected from a publicly available source, but it would be unfair or unreasonable to disclose it in the circumstances

Exception	When the exception applies
	e.g. because it is a child's biometric information, or the disclosure is likely to negatively impact the relevant individual without any reasonable justification.
It is necessary to avoid prejudice to maintaining the law.	Exception **may** apply: • Disclosure upon request: A public sector agency is investigating an offence and requests you disclose all biometric information collected on a certain day, and the request follows all other relevant laws that apply to requesting or obtaining the information. • Proactive disclosure: There is an urgent or exceptional situation, where it is necessary to disclose biometric information to another organisation to avoid a likely risk that a relevant law enforcement agency function would be prejudiced (e.g. to be able investigate serious offending). Exception **would not** apply: • The organisation you disclose the information to cannot take relevant action to avoid prejudice to the maintenance of the law e.g. a potential crime has been committed and you disclose information to another organisation that does not have law enforcement responsibilities. Also see our further guidance on this exception in the Privacy Act.

Exception	When the exception applies
Disclosing the information is necessary to prevent or lessen a serious threat to public health, public safety, or the life or health of any individual.	Exception **may** apply: • There is an imminent and serious threat to someone's safety, and disclosing biometric information you hold (not necessarily about that person) will help the organisation receiving the information respond to and address that threat. For example, disclosing a biometric sample is necessary to urgently locate an individual at serious risk of harm to themselves or others. Exception **would not** apply: • There is a serious threat to someone's safety, but disclosing the biometric information will not help prevent or lessen that threat. Also see our further guidance on this exception in the Privacy Act.
The disclosure is necessary to enable an intelligence and security agency to perform any of its functions. Note: "intelligence and security agency" is defined in the Privacy Act. It means the New Zealand Security Intelligence Service (NZSIS) and Government	Exception **may** apply: • You are complying with a lawful request from the NZSIS or GCSB to disclose biometric information. Exception **would not** apply: • You want to disclose the information to a private security agency (not the NZSIS or GCSB).

Exception	When the exception applies
Communications Security Bureau (GCSB).	
The individual will not be identified when the information is used, or the biometric information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.	Exception **may** apply: • You are disclosing people's biometric information as part of publishing a research study and only information that will not identify anyone will be published. Exception **would not** apply: • You have removed someone's name or their face from their biometric information, but they can still be identified in other ways. • The audience of a publication may have additional knowledge to help them identify an individual in the research. We have more guidance on what makes a person identifiable. While you can rely on an exception to rule 11 in these circumstances, if you are disclosing biometric information for statistical or research purposes, it will usually be good practice to still obtain the relevant individual's authorisation where possible.
The disclosure is necessary to facilitate the sale or other	Exception **may** apply:

Exception	When the exception applies
disposition of a business as a going concern.	• You are selling your business as a going concern (i.e. the company will continue to operate / remain in business after it is sold). Exception **would not** apply: • A potential purchaser is interested in the biometric information you hold but disclosing it is not necessary to facilitate the sale. • You are selling shares in your business but not selling it as a going concern.

Rule 11 Example Scenarios

Collection of voice sample and behavioural biometric information by bank

Exception covered: maintenance of the law

A bank collects a range of biometric information for fraud detection and prevention purposes. It collects a voice sample when customers call the bank call centre. It also collects a range of behavioural biometric information based on how customers interact with the bank's digital services such as internet banking and mobile app.

There is suspected fraudulent behaviour on several customer accounts, and based on the biometric information collected, the bank suspects the fraudulent behaviour on multiple accounts is originating from the same person.

The bank discloses the biometric information it has collected related to the suspected fraudulent activity to the Police to assist the Police in investigating the fraud. The Police would collect and hold the information for this specific purpose and any related investigation of offending. This would be permitted under the "avoid prejudice to the maintenance of the law" exception.

Facial recognition to allow entry to gym

Exception covered: individual authorises disclosure

A gym offers an optional FRT system as an alternative to a physical swipe card for member access. The gym has reciprocal agreements with partner gyms in other cities where each gym, allowing members to access these facilities when travelling. Each gym has its own FRT system and each gym is separately owned and operated.

When an individual chooses to enrol in the FRT system, they are given the option to have their biometric information shared with the other gym(s) that that member may want to use. Provided the gym gives the individual all relevant information (see our rule 3 guidance for more information on informing individuals), this disclosure to other gyms would be permitted under the "individual authorises the disclosure" exception.

Rule 12: Transferring biometric information overseas

Rule 12 is about ensuring that biometric information is adequately protected if it is transferred to a person or organisation based overseas. The general principle is that biometric information must not be disclosed to anyone overseas unless there is protection comparable to that provided under this Code, or another exception applies.

OPC's existing guidance on sending information overseas is also relevant for rule 12. The key difference between rule 12 and IPP 12 in the Privacy Act is that rule 12 requires that biometric information be protected in a way that is comparable to protections set out **in this Code**, rather than those in the Privacy Act.

If your organisation already sends other types of personal information overseas under IPP 12, when assessing whether that overseas jurisdiction provides comparable protection for biometric information, particularly focus on the stricter requirements in rules 1, 3, 6 and 10 in the Code.

Consideration of Māori cultural perspectives, including principles of Māori data sovereignty, are also relevant to your assessment. Notably, rule 1 includes a

requirement to consider cultural impacts on Māori, which forms part of the protections in this Code.

When Rule 12 applies

Rule 12 applies when you are disclosing biometric information to a foreign person or organisation to hold or use the information for their own purposes. It won't generally apply if you are sending information overseas to be held by a third-party service provider solely for storage or processing on your behalf. For example, it wouldn't generally apply if you have a contract with a third-party identity verification provider for new clients (and the third-party doesn't use or disclose the identity biometric information for their own purposes). Our guidance on section 11 of the Privacy Act has more information about using third-party service providers.

We have a decision tree for IPP 12 to help you work out if it applies to your disclosure. You can also use the decision tree to help assess whether rule 12 applies.

Rule 12 does not apply if:

- The biometric information is being sent overseas to the person whose information it is.
- The biometric information is publicly available and it is not unfair or unreasonable in the circumstances to disclose the information outside New Zealand.
- It is a third-party / agent situation, as described above.

When you can disclose biometric information overseas

The first step is to ensure you have a valid ground under rule 11 to disclose the biometric information.

Provided your intended disclosure is permitted under rule 11, you may disclose the biometric information to someone overseas if one of the following applies:

- You specifically tell the relevant individual that the overseas person/organisation may not be required to protect their biometric information in a comparable way to

the Code. After being informed of this, the individual authorises you to disclose their biometric information overseas. E.g. the individual chooses to opt-in to having their voice audio sent and held by the overseas business and on the understanding that it will help train their proprietary voice recognition algorithm.

- The organisation is carrying on business in New Zealand and you believe on reasonable grounds that the overseas organisation is subject to the Code in relation to the biometric information i.e. if it is reasonable to believe that the Privacy Act and Code apply to the organisation receiving the biometric information, then the offshore disclosure is permitted.
- You believe on reasonable grounds that the overseas organisation is subject to privacy laws that provide a comparable level of protection for biometric information as the Code.
- You believe on reasonable grounds that the overseas organisation is required to protect the biometric information in a comparable way to the Code – for example, because of a contract between you and the overseas organisation. Our model contract clauses for IPP 12 can be a starting point for developing a contract, but you will need to adapt them for your use of biometric information and to ensure they are comparable to the **Code**. For example, by covering the rights of individuals to access confirmation of the type of biometric information held about them in rule 6, and the limits on biometric categorisation in rule 10.

There is also an exception in the Code that permits overseas disclosure if you believe on reasonable grounds that the overseas organisation is subject to privacy laws of a prescribed country or a participant in a prescribed binding scheme. However, as at July 2025 there are no prescribed countries or binding schemes. We will update the guidance if there are regulations made to prescribe any countries or binding schemes (the ability to prescribe countries or schemes is with the Governor-General, on recommendation from the Minister of Justice. OPC cannot prescribe countries or binding schemes).

Finally, in some limited situations (for example, if your overseas disclosure is necessary to avoid prejudice to the maintenance of the law or to avoid a serious threat to life or health), rule 12 will not apply if it is not reasonably practical in the circumstances to comply with this rule.

What does comparable protection mean?

Comparable protection doesn't mean that the foreign organisation has to be subject to exactly the same requirements as the Code. But, you need to carefully assess whether any differences are significant.

The foreign organisation may not be subject to requirements that specifically deal with biometrics. If this is the case, you can check their general privacy obligations to make sure the general privacy obligations still provide comparable protection to the Code.

When considering whether the foreign organisation is required to protect the biometric information in a comparable way to the Code, you and your advisors should consider the following factors.

What is the **scope of the overseas privacy law** – does it:

- Cover the foreign person or organisation (i.e. they do not fall within an exemption or carve-out under that law)?
- Cover the biometric information that you provide?
- Take account of the sensitivity of the information that you provide?
- Specifically cover the people whose biometric information you have disclosed (who may not be citizens or resident in that country)?

Other relevant laws:

- Is the foreign person or organisation subject to any laws that are specific to biometrics, artificial intelligence (AI) or automated decision making (ADM)? How

do those laws differ from New Zealand laws? Laws that are more privacy protective than the Code will clearly qualify as “comparable”.

- For Māori biometric information, are there any laws or other protections that apply specifically to indigenous data?
- Are there any laws covering general data fairness, accuracy, bias and discrimination requirements?

Protections:

Will the foreign person or organisation:

- Have security safeguards that are reasonable in the circumstances?
- Dispose of the biometric information securely if they no longer need it?
- Have limits on how they can use the biometric information? (see rule 10). This is particularly important if the foreign person or organisation may use the biometric information for biometric categorisation because of the limits in rule 10. These limits would impact whether there is comparable protection.
- Have limits on how they can disclose the biometric information? (see rule 11 and rule 12 of the Code).
- Be required to notify people about any privacy breach that may cause serious harm, and the relevant data protection body?

Right to **access and seek correction** of biometric information

Will people:

- Have meaningful access to their own information? (including if they are not a citizen or resident of the country the overseas person or organisation is in)
- Be able to request a correction of their biometric information if they consider that it is incorrect?

Accessible and meaningful **complaint processes**

- If something goes wrong, can the affected person make a complaint to a data protection authority?
- Will it be simple and free for a person to access legal remedies?

Independent oversight and enforcement

- Is there an independent data protection authority or Privacy Commissioner in the country that holds oversight, compliance, and enforcement functions broadly comparable to the New Zealand Privacy Commissioner?

You should seek legal advice as necessary to help you decide whether the overseas organisation is required to protect biometric information in an overall comparable way. Note that you may need to use model contract clauses to ensure that protections will follow the information once it is disclosed.

Rule 12 Example Scenarios

Facial recognition to control access to restricted site

A company is using FRT to control access to a restricted site. The provider of the FRT system they choose is overseas and the images and templates will be processed overseas. The New Zealand company ensures that the FRT provider will not use any biometric information that the New Zealand company collects via the FRT system for the FRT provider's own purposes e.g. to train their proprietary algorithm.

Because the FRT provider will not hold or use the information for its own purposes, the New Zealand company is not treated as "disclosing" the information overseas and so rule 12 does not apply. The New Zealand company ensures that their relationship with the overseas provider is managed in a way that is consistent with OPC guidance on third party providers.

Collection of voice sample and behavioural biometric information by bank

A bank plans to use a range of biometric information for fraud detection and prevention purposes. It will collect a voice sample when customers ring the bank call centre. It will also collect a range of behavioural biometric information based on how customers physically interact with the bank's digital services such as internet banking and mobile app (e.g. keystroke logging, mouse and device use).

If the bank is investigating suspected fraud, it may need to send biometric information to its overseas head office. The bank assesses the other country's laws that its overseas agency is subject to and receives legal advice that overall, the overseas head office is subject to laws that provide comparable protection to the Code. In addition, the bank has a contract with its head office that requires the overseas agency to protect biometric information in a comparable way to the Code. Either the fact that the overseas head office is subject to comparable laws or the contract with comparable protections would be enough to meet the rule 12 requirements.

Rule 13: Unique Identifiers

Rule 13 largely replicates IPP 13 from the Privacy Act.

Unique identifiers can be used to easily track individuals across systems, link unrelated datasets about a person, or facilitate identity theft or fraud. There are also clear benefits to organisations in assigning identifiers to efficiently administer their functions. Rule 13 allows the use of biometric information as unique identifiers, subject to certain limits on their use and re-assignment to reduce the risk to privacy.

What is a unique identifier?

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.

A biometric template is a mathematical representation of a biometric characteristic (like a fingerprint) generated by a biometric system. It may look like a unique string of numbers that relate to the biometric characteristic e.g. a set of coordinates.

Biometric templates are capable of being **assigned as unique identifiers**. How organisations use the biometric template and how the biometric system operates will determine whether the organisation is assigning the template as a unique identifier.

When will a biometric template be a unique identifier that is assigned?

Assigning a unique identifier means that you are using a unique identifier (e.g. a number) as the **primary means of identifying a specific person in your systems**. For example, you use it to bring up the person's file or other key information about them.

- For a biometric template to be assigned as a unique identifier, it must be central to how your system identifies and organises information about people.
- Generating a biometric template temporarily (e.g. for a one-time comparison) does not count as assignment.
- Recording a unique identifier to communicate with another organisation about that person is not **assigning** it.

The examples below explain when a biometric template is assigned as a unique identifier.

What controls does rule 13 place on using unique identifiers?

Rule 13 requires that:

- You only assign a unique identifier if it is **necessary** to enable you to carry out your functions **efficiently** (rule 13(1)).

    - Ask: Is assigning a biometric template genuinely needed to help your organisation run smoothly, avoid confusion, or manage your operations more effectively? What other options are there to organise the way you identify individuals in your systems?
    - While this test is more focussed on operational efficiency, if you have determined under rule 1 that using biometric processing is necessary and proportionate, you will likely comply with this rule if your use case relies on using a biometric template to organise the way you identify individuals in your systems.
- You must **not assign the same unique identifier** that **you know another organisation** has already assigned to the same person.
    - This means you must not assign a biometric template that you know has been generated by another agency's biometric system and used as a unique identifier in their system for the relevant person.
    - In practice, this is unlikely to happen unless another agency directly shares a template with you. Differences in biometric systems and variations in the biometric sample used will produce different templates, and two agencies separately assigning different biometric templates to the same person is not a breach of rule 13.
- If you are assigning a biometric template as a unique identifier, you must take reasonable steps to ensure it is **only assigned to an individual whose identity is clearly established**.
    - This requirement helps mitigate the risk of misidentification.
    - You don't necessarily need to know their name or other biographic details to establish the person's identity.
- You must take reasonable steps to **minimise the risk of misuse** of that unique identifier (e.g. to mitigate the risk of privacy breaches or identify theft).
    - For example, by limiting access to the system and appropriately protecting the unique identifier. See rule 5 for more information about safeguards.

- You generally **can't require that an individual disclose their unique identifier**, including when that unique identifier is a biometric template. In practice, this is unlikely to be an issue in most biometrics contexts.

Example 1: Biometric template is assigned as a unique identifier

A retail store is using an FRT system to identify people on a watchlist for staff and customer safety purposes. The retailer generates and records a unique facial template for each person on the watchlist (the reference template). It then uses the reference template to uniquely identify specific people when they enter the store.

In this case, the retailer is assigning the reference templates as a unique identifier because their watchlist system is organised around the reference template as the main identifier for the individual (as opposed to using a name, customer ID or other identifier).

However, the biometric templates generated for individuals walking into the store and used for comparison with the enrolled biometric templates would **not** be assigned as unique identifiers for the purposes of rule 13 (the probe template). They are only used for a one-off comparison, to determine whether the individual entering the store is on the watchlist (and they may be discarded once the comparison has been made).

Is the store complying with rule 13?

The store is permitted to assign the biometric template as a unique identifier and complies with rule 13 if it applies the relevant controls. The main implication of rule 13 is that the unique biometric template is **not transferable to another organisation as their primary means of identifying the person in its systems**. However, another organisation could generate its own biometric template to assign to the same individual.

Example 2: Biometric template not assigned as a unique identifier

A company is using FRT to verify the claimed identity of their customers. They use their biometric system to generate and compare unique facial templates based on the customer's photo in an identity document and a live selfie of that customer. If the

templates are sufficiently similar, above the match threshold, the system will produce a match result.

These facial templates are **not** being assigned as unique identifiers. The company is not using the biometric templates as the primary means of identifying the individual within the company's systems but only for the limited purpose of verifying identity at a point in time.

Biometrics guidance appendix: Applying the Code to example use cases

This appendix contains three examples of how organisations may want to use biometric information. It provides an overview of how the Code could apply to each scenario.

> Note: All the examples in the guidance are simplified and are for illustrative purposes only. They are not an endorsement of any particular biometric system or a comment on any particular purpose or use case. Agencies must conduct their own assessment based on their own circumstances for each use of biometrics. Agencies will require more detail for their assessment than is included in the examples.

Example 1: Using facial recognition to verify customer identities (biometric verification)

Scenario: Novel Investments Ltd has a legal obligation to confirm the identity of their clients. Novel Investments want to use a third-party electronic identity verification provider, Biometric Identity Check Ltd (BIC) to remotely verify the identity of new clients.

BIC validates the identity document (e.g. passport) presented by the new client and uses facial recognition technology to compare the customer's photo in the identity document with a live selfie. The live selfie will be deleted once the client's identity is verified, but a copy of the identity document could be retained if it is necessary to comply with a legal obligation.

Who's responsible if you use a third-party provider?

BIC will be Novel Investments' agent and will not use or disclose the information for its own purposes. Therefore, Novel Investments is responsible under the Privacy Act for the processing carried out by BIC on Novel Investments' behalf and needs to ensure the activity is compliant with the Code. See our guidance on using third party providers for more information.

Rule	Application of rule
Does the Code apply?	Yes. BIC, as Novel Investments' agent, will collect and use biometric information for biometric verification (live selfie video used for facial recognition). Novel Investments is responsible under the Privacy Act.
Rule 1 – Purpose for collection	Novel Investments' **lawful purpose** is to comply with a legal obligation to verify client identities. Novel Investments determines that biometric processing is **necessary** for that lawful purpose. In particular: • **It's effective**: There is a clear link between the biometric processing and Novel Investments' lawful purpose. Novel Investments obtained evidence such as statistics and test performance data from BIC that gives Novel Investments confidence that the biometric processing will be effective in accurately verifying client identities. • **Alternatives**: Novel Investments researched different options for verifying client identities. They are satisfied that the accuracy and efficiency of

Rule	Application of rule
	the biometric based verification, including the advantage of having a mechanism to verify identities remotely, means that there is no reasonable alternative that would be as effective at verifying identities, especially in light of other manual solutions that they have assessed as having more overall privacy risk. However, a manual verification process will be kept as a back-up **option** where a new customer has difficulty using BIC's service or is sensitive about the processing of their biometric information. Manual verification will require customers to travel to one of Novel Investments' offices in person. Novel Investments will adopt reasonable **privacy safeguards**, including: • Obtaining individual authorisation and providing an alternative to biometric processing to support individual choice. • Having sufficient assurances (e.g. through contract obligations) that BIC uses best practice security safeguards. • Monitoring accuracy and performance (e.g. false rejection and acceptance rates, failure to enrol rates). • Deleting the live selfie as soon as the client's identity is verified. • Liveness check to prevent spoofing

Rule	Application of rule

	Novel Investments assesses **proportionality**:
	• The residual **privacy risk** as low based on:
	  ○ Highly accurate system with limited, targeted collection. The live selfie will be deleted as soon as identity is verified.
	  ○ Individual authorisation will be sought and a manual, in-person alternative will be available.
	  ○ Low risk of bias, low risk of chilling effect on protected rights.
	  ○ Implementation of the privacy safeguards above.
	• The biometric verification system provides a medium to high **benefit** that outweighs the privacy risk based on the benefit to Novel Investments in having a more robust, quick, convenient and cost-effective way of verifying client identities (including verifying remotely). This is a private benefit to Novel Investments that substantially outweighs the low privacy risk.
	
	• Novel Investments considers **cultural impacts** on Māori:
	  ○ Novel Investments confirms BIC's accuracy rates for Māori clients are comparable to non-Māori.
	  ○ Novel Investments designs authorisation to comply with the standard of free, prior and informed consent to mitigate potential cultural

Rule	Application of rule
	impacts, including having an alternative to biometric processing available – i.e. choosing manual verification in person. ○ Novel Investments chose BIC over another provider because BIC stores all biometric information on cloud storage services with servers in New Zealand, and this option better reflects the principles of Māori data sovereignty. • **Overall**: The biometric processing is proportionate due to low privacy risk/impact, clear benefits to the clients and the mitigation of impacts/effects on Māori clients.
Rule 2 – source of biometric information	Novel Investments is collecting biometric information directly from the individual. Even though Novel Investments is engaging a third-party provider, because BIC is acting as Novel Investments' agent, this is still considered direct collection and complies with rule 2.
Rule 3 – collection of information from individual	Novel Investments will meet the rule 3 requirements when the client is first onboarded, using a plain language written statement that is included as part of the client application and verbally going through the minimum notification matters (what biometric information and why they collect it, whether there's an alternative, and where more information can be found).

Rule	Application of rule
Rule 4 – manner of collection	Novel Investments is not breaking any laws in the way it collects the biometric information (it's lawful). It considers its manner of collection is fair and not unreasonably intrusive, particularly because they seek individual authorisation and offer an alternative to the biometric verification.
Rule 5 – Storage and security of biometric information	Novel Investments chose BIC because BIC uses best practice security safeguards, such as immediate deletion of biometric information that is not required to be kept, and technical safeguards like encryption of biometric information that is not deleted. Novel Investments also ensures that it has contractual mechanisms in place to give it confidence that the storage and security practices of BIC meet Novel Investments' requirements. Novel Investments conducts regular audits and assurance checks to confirm the security safeguards used by BIC remain appropriate. See our Security and Access controls guidance in Poupou Matatapu and our rule 5 guidance for more information on storage and security of information.

Rule	Application of rule
Rule 6: Access to biometric information	Novel Investments will comply with requests from clients to access their biometric information. Upon request, it will confirm if it holds any biometric information about an individual. Because the live selfie will be deleted as soon as the client's identity is verified, in general Novel Investments will confirm that it only holds a copy of the individual's identity document (if this is still held) and a record of the fact that the client's identity was confirmed by BIC through the biometric verification process.
Rule 7: Correction of biometric information	Novel Investments will comply with requests to correct biometric information. Novel Investments ensures that its arrangement with BIC will allow it to access and correct information in a timely manner, including the ability to add a statement of correction from a customer.
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	Novel Investments has researched the accuracy of BIC's matching process and determined it is acceptable for Novel Investments' purposes (extremely low percentage of false verifications). However, some false rejections (false negatives) may still occur, so Novel Investments ensures there are ways for customers to flag if their identity verification is inaccurately rejected.

Rule	Application of rule
Rule 9: Retention of biometric information	The live selfie will be deleted as soon as the identity is verified. Other biometric information will only be retained for as long as required to comply with Novel Investments' legal obligation to verify customer identities.
Rule 10: Limits on use of information	Novel Investments ensures it only uses the biometric information for the purpose of verifying customer identities and no other purpose, unless an exception applies. The limits on biometric categorisation in rule 10 are not applicable as Novel Investments is carrying out verification not categorisation.
Rule 11: Limits on disclosure of biometric information	Novel Investments (or its agent BIC) will not share the client's biometric information with any other organisation (unless an exception applies).
Rule 12: Disclosure of biometric information outside New Zealand	Novel Investments (or its agent BIC) will not disclose their client's biometric information outside New Zealand.
Rule 13: Unique identifiers	Novel Investments is not assigning a biometric template to clients as their unique identifier, so rule 13 is not engaged.

Example 2: Using fingerprint recognition in multi-factor authentication to protect sensitive information (biometric verification)

Scenario: Secret Information Limited (SIL) holds highly sensitive personal information about clients that some members of staff must access as part of their job. SIL decides to implement a biometric-based multi-factor authentication (MFA) process to protect the information. Staff that need to access the information must present their username, password and scan their fingerprint to access this personal information.

Rule	Application of rule
Does the Code apply?	Yes, SIL is collecting fingerprints (biometric information) to use in biometric verification.
Rule 1 – Purpose for collection	SIL's **lawful purpose** is to protect highly sensitive personal information (organisations are required under the Privacy Act to use reasonable security safeguards to protect personal information). SIL determines that the biometric processing is **necessary** to achieve their purpose. • **It's effective**: There is a clear link between the biometric processing and SIL's lawful purpose. MFA is a widely used way to protect personal information, and there is an evidential basis that fingerprint scanning offers a highly effective form of protection. SIL confirms the effectiveness of the specific MFA system they intend to use, as well as considering the effectiveness of fingerprint scanning for MFA more generally. • **Alternative**: SIL researched different MFA options and the differing levels of security each provides.

Rule	Application of rule
	There are other authentication factors that SIL could use, including both different biometric factors (e.g. iris scanning) and non-biometric factors (e.g. SMS code, smart cards). SIL considers that, for its context, the fingerprint authenticator has advantages over the other non-biometric options, including being resistant to phishing attacks, unable to be lost or forgotten and unlikely to be stolen. It is also more practical to implement than other biometric options like iris scanning or facial recognition and doesn't present accuracy differentials across demographic groups. Overall, there is no reasonable alternative that would enhance security as effectively and also poses less privacy risk. SIL will adopt reasonable **privacy safeguards**, including: • SIL will consult with employees before introducing the system and offer the ability to opt-out of providing biometric information (but then the employee would lose access to the sensitive information). If the consultation reveals significant employee concerns, the organisation will work with employees to resolve or mitigate the concerns before continuing with the fingerprint MFA system. • SIL will only retain a template of the fingerprint scan, not the actual scan, to reduce risks of spoofing and presentation attacks.

Rule	Application of rule

	• SIL will use best practice security measures to protect the biometric information, including having a process in place to audit any access to the fingerprint templates to identify any employee browsing issues.
	• Not linking the fingerprint information with any other personal information of the employee.
	
	SIL assess **proportionality**:
	• SIL assesses the **privacy risk** as low to medium based on:
	  ○ The MFA measure is targeted so fingerprint data will be collected only from those who need to access the sensitive information.
	  ○ The context of the employment relationship increases the intrusiveness of the measure as the power imbalance may mean employees feel coerced into giving their biometric data. To help mitigate this risk, SIL will consult with employees on whether it is practical to allow employees to opt-out of giving their biometric information (but in that case the employee would lose access to the sensitive information and may require changes to their job following the normal employment process).
	
	• SIL considers there is a medium to high **benefit** that outweighs the privacy risk based on:

Rule	Application of rule
	○ The increased level of security benefits SIL (private benefit) by preventing data breaches and unauthorised access, ensures compliance with any legal requirements around security, protects the organisation's reputation, ensures client trust, and reduces financial and operational risks. There is also a benefit to the people whose information is being protected. ○ This benefit substantially outweighs the risk. • SIL considers **cultural impacts** on Māori: ○ As part of SIL's consultation with employees, it will specifically seek feedback on cultural impacts from Māori employees and consider how to address any impacts raised. ○ The biometric system used has a high accuracy rating regardless of skin tone. ○ The fingerprints will be stored locally on each individual's device so no biometric information will leave New Zealand. • **Overall proportionality:** Despite some level of intrusiveness, overall the measure is proportionate due to the heightened need for robust security measures to protect the sensitive personal information. The privacy and employment impact on employees is further mitigated by the safeguards (see above).

Rule	Application of rule
Rule 2 – source of biometric information	SIL is collecting biometric information directly from the individual.
Rule 3 – collection of information from individual	SIL will comply with rule 3 by informing the employees of the purpose of collection, alternative option and consequences for not providing a fingerprint etc. as part of the consultation before using the system. It will also give employees a plain language, written statement at the time that they provide a fingerprint sample and add information to the employee intranet.
Rule 4 – manner of collection	SIL is collecting information in a lawful way. It will not collect any biometric information of children or young people. Consulting with employees and offering an opt-out of biometric processing is one of the ways SIL ensures the manner of collection is lawful, fair and not unreasonably intrusive.

Rule	Application of rule
Rule 5 – Storage and security of biometric information	SIL is using biometric information to protect other personal information. But it still needs to ensure the biometric information is appropriately protected by security safeguards. Examples of steps SIL takes to protect the employee fingerprint information: • Deleting the original samples and only storing the biometric template. • Storing the template locally on the device. • Not linking the fingerprint template with any other personal information of the employee.
Rule 6: Access to biometric information	If an employee requests access to their biometric information, SIL will confirm if it holds a template of their fingerprint (it doesn't hold a scan of the fingerprint because it is deleted after the individual is enrolled in the system and the template is generated). The template may not be extractable (not readily retrievable), so in that case SIL decides it will provide an explanation that it holds a template and what that means so that the employee better understands what information SIL holds about them.

Rule	Application of rule
Rule 7: Correction of biometric information	SIL will comply with requests to correct biometric information. e.g. An employee is consistently having to make multiple attempts at scanning their fingerprint before gaining access and requests their biometric information is updated. SIL organises for the employee to re-enrol and update their fingerprint template.
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	The way in which biometric information is being collected and used by SIL is unlikely to raise issues under rule 8. Collecting the fingerprint samples directly from the employees helps ensure the information is accurate before it is used. SIL will have processes in place to update the information if needed, e.g. if an employee injured their finger resulting in a changed fingerprint.
Rule 9: Retention of biometric information	SIL doesn't need the fingerprint scan to operate the recognition system after enrolling the employee, so SIL will delete it post enrolment. SIL will only store the fingerprint template for as long as an employee requires access to the sensitive information.

Rule	Application of rule
Rule 10: Limits on use of information	SIL will ensure it only uses the biometric information for the purpose of MFA and no other purpose, unless an exception applies. The limits on biometric categorisation in rule 10 are not applicable as SIL is carrying out verification not categorisation.
Rule 11: Limits on disclosure of biometric information	SIL will not share any biometric information with any other organisation (unless an exception applies).
Rule 12: Disclosure of biometric information outside New Zealand	SIL will not disclose any biometric information outside New Zealand.
Rule 13: Unique identifiers	SIL is not assigning a biometric template to customers as a unique identifier, so rule 13 is not engaged.

Example 3: Using facial recognition to control access to a dangerous worksite for health and safety purposes (biometric identification)

Scenario: Busy Machinery Ltd operates a highly dangerous worksite. They are reviewing their processes to keep workers safe and making sure they comply with legal requirements around health and safety. Among other obligations, they need to ensure they have strict access controls so only appropriately trained staff access certain areas/machinery and have an 'live' record of who and how many staff are on site at any one time.

Busy Machinery decides to explore using facial recognition technology (FRT) to monitor access controls and keep a log of workers on site. The FRT system would have two groups enrolled – workers allowed to access the general worksite area and workers allowed to access certain areas and machinery. FRT would be used to detect workers entering the site and restricted areas and alerts would go off if unauthorised people or workers tried to enter the worksite or restricted areas. The system would also count and record how many workers and who were on site so there was a live attendance log in case of an incident.

Rule	Application of rule
Does the Code apply?	Yes, Busy Machinery is collecting facial images to identify people using a biometric system.
Rule 1 – Purpose for collection	Busy Machinery's **lawful purpose** is to put in place a more robust process to keep workers safe and comply with legal health and safety requirements. Busy Machinery determines that the biometric processing is **necessary** to achieve their purpose. • **It's effective**: There is a clear link between the problem (needing a way to monitor and restrict who accesses the worksite and uses the machinery) and the ability of an FRT system to help solve the problem. The FRT provider Busy Machinery chose has deployed this type of solution in similarly dangerous work environments before and has data showing how it worked, how it can help in the event of a health and safety incident, as well as a reduction in unauthorised access to restricted areas. The facial recognition algorithm chosen has a high accuracy rating across

Rule	Application of rule
	demographics and could be set to an appropriate specificity and sensitivity level that balanced false negatives (disrupting workflows) and false positives (guarding against unauthorised people). • **Alternatives**: There are other ways for Busy Machinery to monitor workers on site and control access but these all had significant drawbacks. It was important for Busy Machinery to find a seamless 'contactless' way of monitoring each worker entering and exiting. Busy Machinery considered a physical access card option or sign on in a paper register at the site entrance, which were feasible options but were likely to be less effective as they rely on workers to remember cards or to sign in. Workers are usually wearing physical protective suits and/or carrying equipment that would make using these alternatives more difficult and less convenient. Cards can also be passed from an authorised user to an unauthorised user, creating safety and security risks. Therefore, Busy Machinery determines that it cannot reasonably achieve its purpose as effectively by an alternative means with less privacy risk. Busy Machinery will adopt reasonable **privacy safeguards**, including: • There will be a strict policy around access to and use of data, backed up with robust access and audit controls. Information from the FRT system will only be

Rule	Application of rule

	used for health and safety and incident responses, not performance, disciplinary actions, or covertly watching employees.
	• The daily log of data collected will be deleted as soon as the site manager confirms that there was no health and safety incident.
	• Providing for human review and oversight of the system i.e. the worksite manager will review any decisions flagged by the workers as wrong.
	• The system will be regularly reviewed to ensure it is sufficiently effective and information is adequately protected.
	• Busy Machinery consults with workers about the FRT system as well as the other non-biometric options. The outcome of the consultation was that the workers were comfortable with the FRT system as long as above safeguards adopted.
	
	Busy Machinery assesses **proportionality**:
	• This system poses moderate **privacy risk** but the **residual risk** level is lower due to the safeguards implemented:
	  ○ Monitoring a workspace using FRT that records live attendance onsite is generally more intrusive than the use of CCTV.
	  ○ The context of the employment relationship and power imbalance increases the intrusiveness of the measure as employees may feel a lack of

Rule	Application of rule
	control or choice, surveilled by their employer or concerned about use for other employment purposes. ○ There is some risk of scope creep as information collected for safety purposes could be useful for other employment purposes (monitoring performance, time management, disciplinary actions), even if not part of the original reasons for using the system. ○ Everyone who enters the worksite will be scanned, including those who accidentally enter. There will not be an opt-out/alternative set up because it would undermine the integrity of the system. ○ There is a possibility of false negatives which could be disruptive or alarming for a worker who would have to then challenge the automated decision. Busy Machinery will need to provide a way for human oversight and review of any automated alerts. • Busy Machinery considers the **benefit** outweighs the residual privacy risk: ○ The benefit to Busy Machinery from improved management of health and safety risks and a reduction in unauthorised access justifies the privacy risk posed by the system. The importance of improved health and safety helps

Rule	Application of rule

	mean that this benefit substantially outweighs the privacy risk.
	
	• Busy Machinery considers **cultural impacts** on Māori:
	  ○ Some workers are Māori and wear moko, so there is culturally sensitive/tapu information that will be captured by the FRT system (even though the FRT system will not be analysing the moko specifically).
	  ○ The FRT system will not be optional and there will be no opt-out, which could raise tikanga issues around obtaining free, prior informed consent and giving people control over their own information.
	  ○ Busy Machinery decides to engage with all staff about the design of the system and specifically asks for feedback on potential cultural impacts so these can be addressed.
	
	• **Overall proportionality:** Busy Machinery considered the safeguards would meaningfully lower the overall risk and intrusiveness of the proposal to a level that would make the measure proportionate when weighed against the benefits and cultural impacts.

Rule	Application of rule
Rule 2 – source of biometric information	Biometric information (face image) is collected directly from the workers to enrol them in the database and a face image is captured for comparison each subsequent time they enter the worksite. Remote collection (e.g. by a FRT camera) is still considered direct collection for the purposes of rule 2.
Rule 3 – collection of information from individual	Busy Machinery will comply with rule 3 by informing the workers of the purpose of collection, no alternative option etc. as part of the consultation before using the system. It will also give workers a plain language written statement at the time that they enrol in the system. Any new potential workers will be fully informed about the system before starting work. A sign will also be installed at the entrance to the site so that anyone new to site also receives the information required by rule 3. Having a sign also reminds workers of the system operation and mitigates the need to re-notify them if they haven't been to site in a while.

Rule	Application of rule
Rule 4 – manner of collection	Busy Machinery is collecting information by lawful means. It does not expect to collect any biometric information of children or young people. Consulting with workers and ensuring good transparency around when and how the biometric information is collected is one of the ways Busy Machinery ensures the manner of collection is lawful (e.g. compliant with obligations in employment law), fair and not unreasonably intrusive. It will also ensure cameras are not stationed at any areas where sensitive information, or information that is not necessary, would be collected – for example, no cameras in or pointing at the break room or bathrooms.
Rule 5 – Storage and security of biometric information	Examples of steps Busy Machinery takes to protect the biometric information: • Robust access and audit controls for information collected through the FRT system. • Deleting daily log of data once there is confirmation of no health and safety incident. • Not linking information collected through the FRT system with any other personal information of workers. • Strong technical protections for biometric information.

Rule	Application of rule
Rule 6: Access to biometric information	Busy Machinery will comply with requests from workers to access their biometric information, including letting them know that they hold both a face image of the worker's face and a biometric template created from the image.
Rule 7: Correction of biometric information	Busy Machinery will comply with requests to correct biometric information. For example, a worker might request to add a note to the system stating that they have an identical twin.
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	The way in which biometric information is being collected and used by Busy Machinery is unlikely to raise issues under rule 8, provided the system as a whole is operating at a highly accurate level.
Rule 9: Retention of biometric information	Busy Machinery will delete the daily log of data once there is confirmation of no health and safety incident. The photos of workers and face templates will be deleted once the relevant worker no longer requires access to the site as part of the off-boarding process.

Rule	Application of rule
Rule 10: Limits on use of information	Busy Machinery plans to only use the biometric information for the original purpose it collected it for and no other reason (as outlined in its strict FRT policy). The limits on biometric categorisation in rule 10 are not applicable as Busy Machinery is carrying out biometric identification not categorisation. However, as an example, if Busy Machinery wanted to detect or infer information about workers from their faces as part of their health and safety approach (e.g. to monitor attention or distraction), Busy Machinery would need to ensure it was compliant with the biometric categorisation limits and that doing so was necessary and proportionate.
Rule 11: Limits on disclosure of biometric information	Busy Machinery may need to disclose information about a health and safety incident to a regulatory body such as Work Safe. This would likely be permitted under the exception that allows disclosure for a directly related purpose. Busy Machinery includes this possibility in the information it gives workers under rule 3. Busy Machinery does not intend to make any other disclosures to any other organisations (unless an exception applies).
Rule 12: Disclosure of biometric information outside New Zealand	• Busy Machinery will not disclose biometric information outside New Zealand.

Rule	Application of rule
Rule 13: Unique identifiers	Busy Machinery will not assign a biometric template to employees as a unique identifier, so rule 13 is not engaged.