Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing

Privacy Code draft guide – rule 3

Privacy Commissioner
Te Mana Mātāpono Matatapu

Contents

Rule 3: Tell people about the information you collect

Rule 3 is about ensuring people understand, at the time of collection or as soon as possible after the biometric information is collected:

- What information is being collected.
- Why it is being collected.
- If the individual must provide the information, and if so, why (e.g. because of a particular law).
- Who will receive the information.
- Who to contact in relation to the collection of the information.

What you need to tell people

There are several things you need to tell people if you are collecting biometric information.

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. Express it in non-technical terms wherever possible e.g. “a scan of your fingerprint” not “a biometric sample”

What you need to tell people	Guidance or example
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 operate a facial recognition system to detect when individuals on a watchlist enter our premises and monitor their actions”, not “for business use” or “for general security”.
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.
The intended recipients of the biometric information.	Let people know everyone who will have access to their biometric information. This is especially important 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.

What you need to tell people	Guidance or example
The name and address of who will collect and hold the biometric information. Also include 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.	Give people the contact details that you would like them to use if they have any questions about biometric information. See our rule 6 guidance or our IPP 6 and IPP 7 guidance for more information about access and correction requests. Information about submitting a complaint is available on our website.
If there is a law that requires or allows you to collect 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.
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?
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. 2 years after the person stops using the service).

What you need to tell people	Guidance or example
How the person can raise a concern about biometric processing, including the handling of their biometric information, and how they can make a complaint about the handling of their biometric information	If you expect people to follow a particular process (e.g. using a specific form), make that easily available to them.
If you know of any laws that could affect how the person's biometric information is used or disclosed.	For example, if there is a New Zealand or overseas law that requires or allows the biometric information to be used or disclosed.
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 rule 1 guidance on effectiveness 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. Those 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 these matters, you must communicate them 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

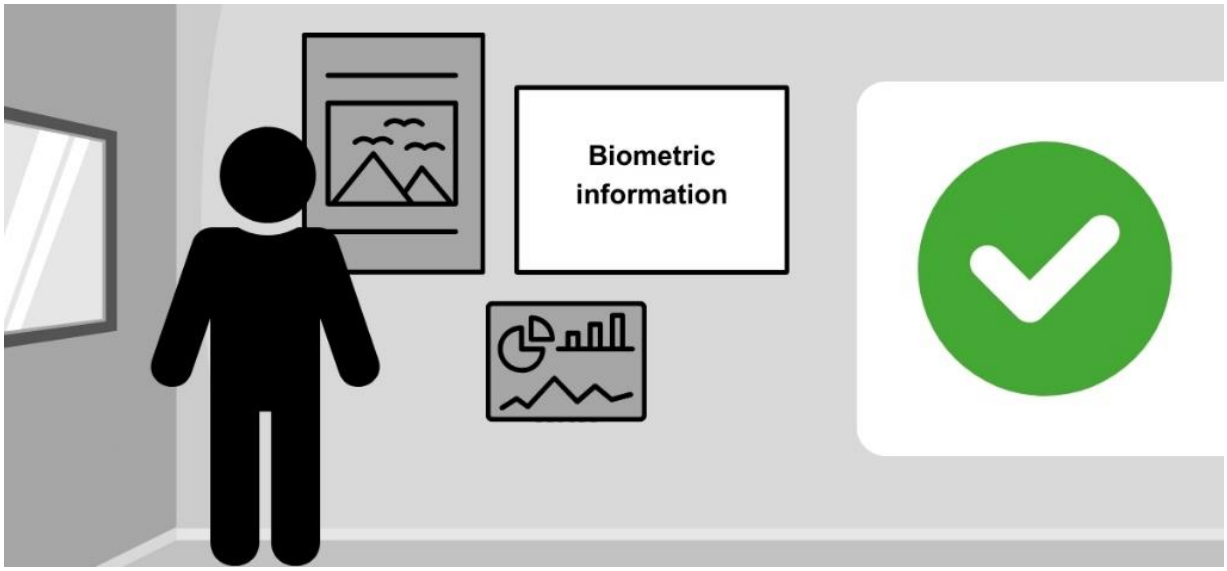
Clear and conspicuous means information should be obvious, accessible, easy to understand and set apart from other information.

For example, you could:

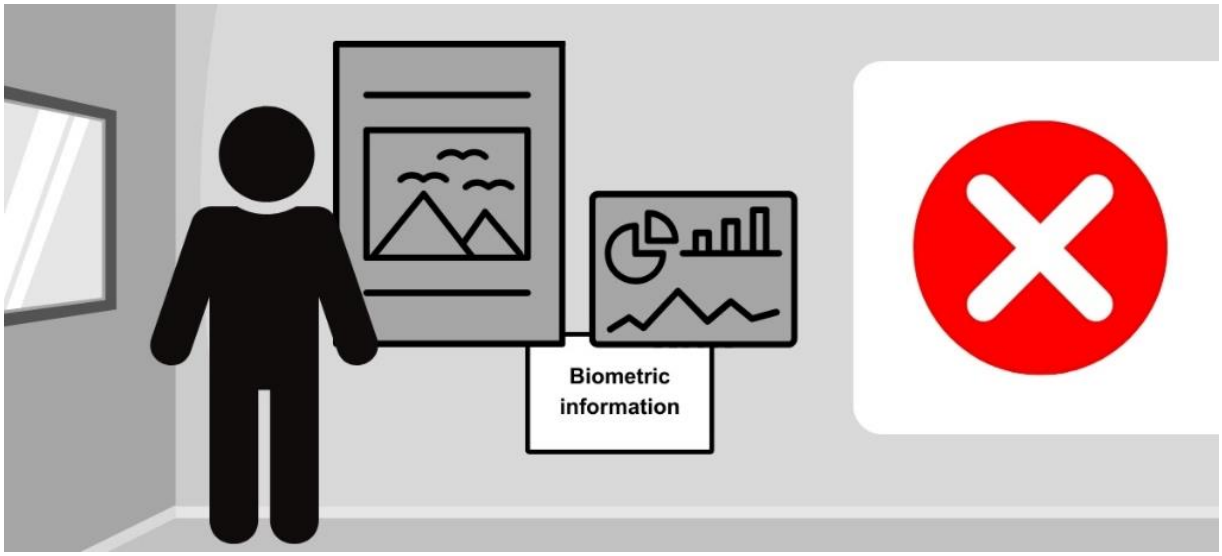
- Ensure any signs or website content are large enough to draw people's attention, easy to read, distinguishable from other signs e.g. promotional signs, and placed apart from other signs so that the biometric information isn't lost among all the other information.
- Ensure verbal notices given by staff to people are clear and limited to information about biometric information (i.e. not part of a longer presentation about unrelated matters).
- Play an audio notice that is clear, easy to understand and set apart from promotional or other messages through the tone, introduction or manner of presentation.
- 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:

- **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. But if it was every 6 months, then it could be appropriate to remind the person each time.
- **How are you telling people about the rule 3 matters?** For example, methods like signs or website content would justify more frequent reminders (or having the signs/website content continually present). Whereas if you are telling people through a one-on-one conversation with a staff member, this probably wouldn't require as many reminders.
- **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 should inform the person of all the rule 3 matters each time you collect their information.

How to tell people

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

- 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.
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.

Exception to rule 3	Note on when the exception applies
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 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

Facial recognition for access to an apartment building

A body corporate for an apartment building wants to implement an optional FRT system as an alternative to swipe cards/keys for access for building residents. The system will be mounted in a specific place and when someone wants access, they push a button to activate the camera.

The body corporate will send an initial email to all residents explaining the system and asking individuals to consider whether they would like to opt-in to the system. Then before the body corporate collects any biometric information, it will send another email to all residents that includes an attachment with detailed information about the rule 3 matters.

The body corporate will also attach a notice next to the FRT camera for the facial recognition system. The notice could say:

> Facial recognition camera: collects facial images to allow access to the building. You may use a swipe card as an alternative. For more information email [email address].

The body corporate will send annual reminders to residents about the FRT system that covers all the rule 3 matters.

Fingerprint scan for Multi Factor Authentication (MFA)

An employer plans to implement fingerprint scanning as a form of MFA for employees who have access to a database with highly sensitive information.

Before collecting employee fingerprints, a manager will talk with each employee about how their information will be collected. They will also provide them with a copy of the information in writing. Information will also be posted on the employer intranet.

The employer does not need to tell employees about the rule 3 matters every time the employee scans their fingerprint.

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 call the bank call centre. It will also collect a range of behavioural biometric information based on how customers interact with the bank's digital services such as internet banking and mobile app.

When people call the bank, there will be a recorded message about the collection of their biometric information. In addition, on the bank's website home page, there will be a quick link to further information about the use of biometrics.

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 persons who have self-excluded or otherwise been 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].