Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing

Privacy Code draft guide – rule 2

Privacy Commissioner
Te Mana Mātāpono Matatapu

Contents

Rule 2: Source of biometric information

Rule 2 of the Code is about the source of biometric samples – where you collect the information from. Unless an exception applies, you must 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 sample from someone to use in a security access system.
- You collect a voice sample from a customer when they call your call centre for fraud detection and prevention purposes.
- You collect images from your existing 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 know that their biometric sample is being collected, you are still collecting it directly from the individual.

Collection that is not direct could look like:

- You pay for access to a database of facial images of customers to use in your facial recognition system.
- You obtain a biometric sample of one of your employees 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.

All the exceptions require you to have a reasonable belief that the exception applies. Because biometric information is inherently sensitive, what is reasonable in the circumstances can be a higher standard than what would be reasonable in circumstances with less sensitive information.

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.

For some exceptions, such as where direct collection would be detrimental to the individual, it could be appropriate to ask the individual for their view (unless asking

them would be detrimental to their mental health or wellbeing). For example, if you believe that direct collection would be inconvenient (as opposed to harmful) for the individual, you should ask the individual for their authorisation to collect the sample from someone else, rather than relying on the "prejudicial to the individual" exception. But, for other exceptions, such as where direct collection would prejudice the purpose of collection, asking the individual would not be appropriate.

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: • You know that someone would be harmed if you collected the biometric sample directly from them. For example, someone has a mental or physical health condition that means it would be harmful for you 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: • You assume it would be prejudicial to the individual's interests, but you don't have any good evidence about why.

Exception	Note on when the exception applies
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: • You are collecting biometric samples for fraud investigation and collecting the information directly from the individual would undermine your investigation. Exception would not apply: • It is less practical for you to collect the information directly from the individual, so you don't want to.
The individual authorises the collection from someone else.	Exception may apply: • 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: • 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:

Exception	Note on when the exception applies
	• 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: • You are collecting a biometric sample from photos on social media that require you to have additional permission to view the photos (such as being a friend or a follower of the social media account).
It is necessary to avoid prejudice to maintaining the law.	Exception may apply: • 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:

Exception	Note on when the exception applies
	• 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 offending is the purpose of your biometric processing that meets rule 1, then you can likely use other exceptions under rule 2).
The overall circumstances mean you cannot comply with rule 2 for the particular case.	Exception may apply: • 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 would not apply: • 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: • 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: • 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.

Exception	Note on when the exception applies
	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 to allow entry to a gym

Topics covered: direct collection, publicly available information, individual authorisation, social media

A gym plans to use FRT as an alternative to a physical swipe card to provide access to its members. The gym asks members who want to opt-in to the facial recognition system to come to the gym at certain times where a staff member will take a photograph (the biometric sample) to enrol in the system (direct collection).

Some members want to opt-in but they cannot come at the specific times where the staff member will be taking photographs. For those members, the gym will ask the members to send in a photo directly or ask for their authorisation to collect a photo from the individual's public social media accounts.

The gym considers collecting photos from members' social media profiles under the publicly available information exception. But, even though some photos may be publicly available, the gym recognises that best practice is still to collect the information directly, or seek authorisation from the individuals to get their images from social media, given the sensitivity of facial recognition systems and the importance of maintaining trust with their members.

Facial recognition for access to an apartment building

Topics covered: individual authorises indirect collection, direct relationship with individuals

The body corporate for an apartment building plans to use FRT as an alternative form of access to the building. It asks residents who want to opt-in to the FRT system to provide a photograph (the biometric sample) to enrol in the system (direct collection). Each resident is emailed a unique link to submit their photograph so that the body corporate can ensure the individuals each provide their own photo, rather than one person providing a sample for other people they live with, which could be indirect collection.

Some residents of the building also want to enrol their friends or family who are frequent visitors to the building. They suggest they could send a photo of their friends or family to the body corporate to be enrolled in the system. Because the body corporate does not have a direct relationship with the non-resident individuals, it would be difficult to have reasonable grounds to believe that the non-resident individuals authorised the indirect collection. Therefore, the body corporate only enrols people who can provide a photo directly through their unique link.

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 photos from 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 prejudicial 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.

A note on the "prejudicial to the individual's interests" exception

Note: You should consider asking the individual for their view about whether collecting information directly 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.

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.