Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing

Privacy Code draft guide – rule 6

Privacy Commissioner
Te Mana Mātāpono Matatapu

Contents

Rule 6: Access to biometric information

Rule 6 is about an individual's right to access information you hold about them. In general, an individual has the right to receive:

- 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 of the Code).

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.

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. An example of a processing result includes confirmation of a match arising from a verification process or an age range estimate as a result of 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 are the same and you can provide them to the individual at the same time. If you don't know what information the individual is seeking you should ask the individual to clarify.

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 (e.g. numerical representation of their facial features or fingerprint ridges)..

The requirement to confirm the type of biometric information you hold is in the Code because it may be difficult to provide someone with meaningful 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 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, you should also provide a description of the information held. The description does not need to describe the biometric information in highly technical terms, but you should provide enough detail to help the individual understand what biometric information you hold about them and, if relevant, why you cannot provide a copy of the information. Describing what the information is used for in the system can be helpful.

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, with 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

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

If the biometric information cannot be 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.

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. In that case, 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.

OPC has more 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.

You don't need to retain biometric samples just to respond 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. But, you should not delete any biometric information that is otherwise appropriate to retain to prevent people from being able to request access to it.

Rule 6 Example Scenarios

Facial recognition to allow entry to a gym

Topics covered: confirmation of type of biometric information and access to results of the biometric processing

A gym uses a facial recognition system as an alternative to a physical swipe card to provide access to its members. The gym receives a request from an individual for access to their biometric information and for access to a list of times when that individual accessed the gym (the results of the verification process).

Once an individual enrols in the facial recognition system, the system processes the enrolment photo (the biometric sample) into a biometric template and deletes the biometric sample. So, the gym holds a biometric template and a log of times the system has allowed the individual to enter the gym because of a match against the biometric template (a list of biometric results).

The gym confirms that it holds a biometric template of the individual. It is not possible to extract the template from the system, so the gym confirms it holds a biometric template and provides a brief explanation of what that means. It also provides a screenshot of the access log (the record of results from the biometric identification). The access log is treated as an IPP6 request rather than a rule 6 request, but this does not make any practical difference because the process for responding to an IPP6 request is the same as a rule 6 request, the gym provides this information at the same time as the information about the biometric template.

Facial recognition for access to an apartment building

Topics covered: no information held

The body corporate for an apartment building uses a facial recognition system as an alternative form of access to the building. It receives a request for access to biometric information from a non-resident.

The facial recognition system used by the apartment building automatically deletes any images of people not enrolled in the system. Therefore, they confirm that they do not hold any biometric information of the non-resident individual.

Fingerprint access for Multi Factor Authentication

Topics covered: access to biometric template

A business is using a MFA system using employee fingerprints. An employee makes a request for biometric information. The employer holds a biometric template of the fingerprint that the system uses to verify the employee's identity. It is possible to extract the biometric template from the system, but it is not something that would be readily understandable.

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