Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing

Privacy Code draft guide – rule 1

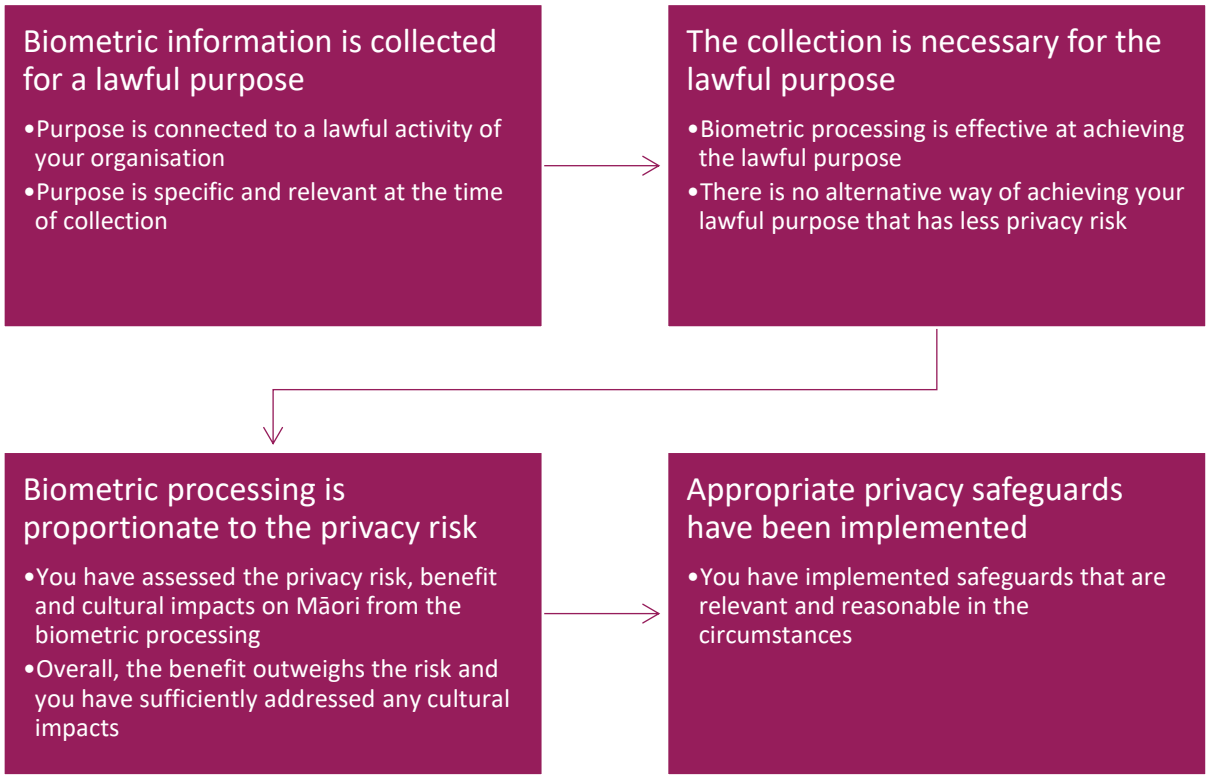
Privacy Commissioner
Te Mana Mātāpono Matatapu

Contents

Rule 1: Purpose of collection

Rule 1 is about your purpose for collecting biometric information. You need to ensure:

- Your collection of biometric information is for a lawful purpose.
- Your collection is necessary for that lawful purpose, meaning it is effective and there is no alternative with lower privacy risk.
- Your biometric processing is proportionate.
- You have implemented appropriate privacy safeguards.



Lawful purpose

It's important for you to identify a clear purpose for why you are collecting biometric information. Identifying a clear purpose will ensure you can properly assess whether the collection is necessary and proportionate, and what privacy safeguards are appropriate. It will also help ensure you can comply with the other rules in the Code.

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 information just in case you may want to use it later.

The purpose also 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.

Necessary for lawful purpose

Biometric information may only be collected if it is necessary for a lawful purpose that is connected with a function or activity of your organisation.

For the collection 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. This requires that the collection is both effective in achieving your lawful purpose, and that there isn't an alternative means that would have less privacy risk.

The fact that biometric processing is available, convenient or desirable for you to use is not enough to show that the collection of biometric 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.

Effectiveness is about whether and to what extent the biometric processing achieves your specific lawful purpose, not 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.

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 by an alternative means with less privacy risk and to the benefit of your processing, which forms part of the proportionality assessment (see our guidance on benefit at page 34 of the full guidance).

Effectiveness is an ongoing requirement. You need to ensure that your processing remains effective once the system is in place.

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 from vendor or independent body.
- 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 use case.
- Evidence about the scientific or technical validity of overall process to address the issue/problem.
- Running tests or simulations on training data.
- 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).
- Expert opinion(s) and academic or scientific research.
- Customer surveys to gain understanding of customer desire for improvements in experience/efficiency etc.

Running a trial to assess effectiveness

The Code allows you to run a trial to assess whether your biometric processing will be effective in achieving your lawful purpose, provided all the other requirements of rule 1 are met. That is, the collection is for a lawful purpose, there are no alternatives with lower privacy risk, the collection is proportionate and appropriate privacy safeguards are in place.

The biometric processing 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.

A trial must not run for any longer than is necessary to show effectiveness. Before establishing the trial, you need to notify how long the trial will go for. 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. 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 need to stop collecting biometric information.

During a trial, you need to comply with all obligations in the Code, for example notification requirements (rule 3) and requests from individuals to access or correct their biometric information (rules 6 and 7). OPC can still investigate any complaint brought by an individual about a breach of one of the rules in the Code or otherwise use our compliance powers under the Privacy Act during a trial period. You must notify OPC of privacy breaches during the trial in accordance with the Privacy Act. You are also accountable for any privacy harm caused to individuals during a trial period.

You should consider whether it is appropriate to take adverse actions against individuals during a trial. In some cases, it will not be possible to gain evidence on effectiveness without taking adverse actions. 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.

> 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).

No alternative with less privacy risk

If you can achieve your lawful purpose through an alternative with less privacy risk, then your biometric processing is **not necessary**. More information on assessing privacy risk is included in the privacy risk section at page 8 of this rule 1 guidance.

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 lawful 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 **does not need to achieve the exact same outcome** as the biometric processing for it to be a viable alternative. It is an overall assessment of whether an alternative with less privacy risk would be able to achieve your lawful purpose to a sufficient degree. If so, the biometric processing is not necessary. But, if there is no alternative that would be able to achieve your lawful purpose to a sufficient degree, that can help you show that your biometric processing is necessary.

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 from your use of biometrics. Privacy risk is the risk that the privacy of individuals may be infringed by the biometric processing, and it includes a range of impacts on individuals. Note that the concept of privacy infringement is broader than interference or breach and incorporates actions that may limit, undermine or encroach on an individual's privacy or deter individuals from exercising their rights. When considering

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

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.

The privacy risks listed in the Code are:

- 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 agency.
- 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 agency. "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.

How to assess privacy risk

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

When assessing the privacy risk of your biometric processing, you should consider **what** information you are collecting, **whose** information it is, **why** you are collecting it, and **where and how** you are collecting it.

Each aspect of what, who, why, where and how has some inherent or unmodifiable risk factors. These factors cannot be modified to become lower risk. For example, in almost every situation, collecting children's information will have a higher privacy risk than collecting the same information from adults. Similarly, collecting information for public surveillance purposes will almost always be higher risk than for highly targeted 1:1 identity verification purpose.

There are also some modifiable risk factors, which can be modified to become lower risk. For example, how much information you collect and the way you collect, protect, use and disclose it. You could design the biometric system in a way that increases or decreases the amount of information collected and stored, with a corresponding increase or decrease in risk. Similarly, broader use of biometric information will increase the risk, whereas highly limited use of the information will generally decrease the overall risk.

Questions to ask to assess risk

What

- What information are you collecting?
- How sensitive is the information you are collecting?
- How much information are you collecting? (more info, higher risk)

Who:

- Whose information are you collecting?
- How many people are you collecting from?
- Are the people whose information you are collecting vulnerable in some way? For example, are they children? Are they experiencing distress?
- Is there a power imbalance between you and the people whose information you are collecting? (consider – employer/employee, landlord/tenant, government agency with enforcement powers etc., a provider of critical service with few alternatives vs. a provider of non-critical service with lots of alternatives).
- Are the people whose information you are collecting more likely to suffer from issues with bias or discrimination? For example, Māori, minority groups, disabled people?
- Have individuals freely authorised the collection?
- Have you consulted with people whose information will be collected?

Where

- What is the context for collection – public space, private space, retail, entertainment?
- Are there realistic alternative options if individuals want to opt out of biometric processing?

Why

- What is your purpose for collecting information?
- How complex is the use case?
- What are the consequences for individuals from the use of the system generally, as well as from any errors or inaccuracy of the system?

- How likely is it that your collection of biometric information may deter people from exercising their protected rights, or reduce the ability of individuals to avoid monitoring where they may not expect to be monitored? (For example, use of biometric systems in public spaces).

How

- How does the biometric system operate?
- How and where is information stored? What information is stored?
- How long is information retained?
- Where is the system physically operating?
- Who has access to information?
- What safeguards are in place?

Risk matrix

Risk matrix	Lower risk	Medium risk	Higher risk
What	• Less sensitive biometric information		• Particularly sensitive biometric information • Multiple types of biometric information collected (e.g. facial images and gait analysis)
Who	• Little to no power imbalance between individuals and agency (e.g. a provider of an optional commercial service with lots of competitors)	• Some power imbalance between individuals and agency • Medium impact on individual if a privacy risk eventuates	• 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.) • No authorisation, unclear authorisation, or

Risk matrix	Lower risk	Medium risk	Higher risk
	• Individual authorises use on a clear opt-in basis, with a genuine alternative easily available to them • Low impact on individual if a privacy risk eventuates		authorisation relied on without genuine alternative. • High impact on individual if a privacy risk eventuates • Vulnerable individuals • Individuals more likely to experience negative impact from system showing bias or discrimination • Involves any information sharing between agencies
Why	• 1:1 verification • Biometrics used for recognition	• 1:N verification • Small or medium database of references • Retrospective or static analysis • Established uses of inferential biometrics with robust scientific basis and high accuracy	• 1:N identification • Large database of references • Use in public spaces • Live recognition • Using biometric processing for secondary purposes wider than just recognition e.g. public safety, crime prevention. • Emerging or novel uses of inferential biometrics. • Use in surveillance/monitoring/ profiling
How	• High quality biometric probes/references • Highly accurate system • Best practice security safeguards	• Information transferred overseas	• Low quality biometric probes/references • Overall operation of the system has wide scope

Risk matrix	Lower risk	Medium risk	Higher risk
	• Overall operation of the system is highly targeted or limited in scope		

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.

Assessing the overall risk requires you to consider the biometrics system as a whole and the context in which your biometric processing will take place. In most cases, if you have any factors from the “higher risk” category, then your system will be higher risk. However, the “how” part of the risk matrix is a key way you can reduce or mitigate the risks to ensure the overall processing is proportionate. The modifiable risk factors (such as what information is collected), are another way to mitigate the risk by changing how the system operates.

Benefit

Part of the proportionality assessment is a weighing exercise between (1) the benefit of achieving the agency’s lawful purpose by means of biometric processing and (2) the scope, extent and degree of privacy risk. This section discusses the benefit and weighing portion of the assessment; more guidance on risk is included in the Privacy risk section.

There are three types of benefits that you can take into account – a public benefit, a benefit to the individuals whose biometric information you are collecting, and a

private benefit to the organisation collecting the biometric information. Each benefit type has a slightly different requirement 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 the public as a whole – for example, improved public safety.
- 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.

Your biometric processing only needs to have one of the three above benefit types. But, if your biometric processing has multiple benefit types, this can strengthen the overall benefit in the proportionality assessment – that is, if your use of biometrics benefits both individuals and your organisation, this will carry more weight in the proportionality assessment than if it only benefitted your organisation.

Assessing the benefit

When assessing the benefit of achieving your lawful purpose, you need to be clear on the specific benefit you expect to achieve, the weight or significance of that benefit, and the expected scale or scope of the benefit. The benefit will be impacted by the effectiveness of the biometric processing – more effective processing will generally provide more benefit than less effective processing. (See also the section on effectiveness).

You should clearly document the benefit. Like your lawful 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”, “increased efficiency”, or “improved safety” – be clear on the actual specific improvement and how it will be achieved through biometric processing. You need to explain what the problem is you are trying to solve, or what the alternative would be without the biometric processing.

Examples of specific benefits:

- 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.
- 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.
- Improved ability to monitor and enforce Exclusion Orders for problem gamblers by using a facial recognition system that will assist staff to identify people with an active exclusion order, rather than relying on memory.

You should use your effectiveness assessment to determine 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 based on your effectiveness assessment, you should have a general idea of whether the biometric processing will offer a small, medium or large scale of the benefit – e.g. a moderate improvement in customer safety or a small increase in security of information access.

Does the benefit 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 type of benefit (public benefit, benefit to the individual whose information is collected or benefit to the organisation collecting the biometric information).

In general, our view is that benefits related to increases in health and safety or reduction in harm or offences will carry a higher weight for the benefit assessment, provided the scale of the benefit is sufficient. In contrast, increases in business efficiency, productivity and customer experience will generally only have a low to medium weight, depending on the scale of the benefit. A small increase in business efficiency would only carry a low weight relative to the privacy risk, whereas a small increase in public safety could still carry a moderate or high weight depending on the overall circumstances.

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.

It requires an overall assessment to answer the question of whether the benefit gained is proportionate to the privacy risk from the biometric processing. If your overall privacy risk is high, you will need a correspondingly high/strong benefit for the overall processing to be proportionate. If your overall risk is low, then even with a small benefit the processing could still be proportionate. If your risk is high but your benefit is only low or moderate, 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.

Cultural impacts and effects on Māori

Part of the proportionality assessment is considering the cultural impacts and effects on Māori. Negative cultural impacts and effects which you do not address may mean the overall biometric processing is not proportionate. Cultural impacts and effects could result from cultural perspectives (e.g. tikanga Māori, Māori data sovereignty) that affect how Māori view or are impacted by biometric processing. It could also come from any different impact the biometric processing has on Māori, for example discrimination against Māori because the biometric processing 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 managed. From a Māori perspective, tikanga such as tapu, whakapapa, mauri, noa, mana and utu regulate how you collect, store, access, maintain and disclose biometric information.

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 impact the tapu, mana and mauri of the injured 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.

An example of a specific cultural concern for Māori is capturing images of moko (traditional tattooing), 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.

Crown agencies need to consider any use of biometric information in the context of te Tiriti obligations. For example, how do principles such as tino rangatiratanga and partnership impact the use of Māori biometric information?

Principles of Māori data sovereignty are another cultural imperative that influences the way that Māori view biometrics and can help all agencies (Crown and non-Crown) consider how the use of Māori biometric information could impact and affect Māori.

Definitions for key concepts

The definitions below come from *Māori data sovereignty and privacy.* Tikanga in Technology discussion paper. Hamilton: Te Ngira Institute for Population Research – Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., Muru-Lanning, M., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D. & Sterling, R. (2023).

- **Mātauranga Māori:** Māori knowledge systems and ways of knowing.
- **Mauri:** life force.
- **Noa:** unrestricted, be free of tapu.
- **Taonga:** those things and values that we treasure, both intangible and tangible.
- **Tapu**: sacred, restricted or prohibited.
- **Tikanga:** values and practices for proper conduct.
- **Whakapapa:** genealogy; lineage.
- **Whānau, hapū and iwi:** family, sub-tribe or clan, and tribe (respectively).

Considering and addressing cultural impacts

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. A failure to adequately identify or address cultural impacts and effects may undermine the reasonable belief that the biometric processing is proportionate.

What this requires in practice can change depending on your specific use case and context, but it does require agencies to make a reasonable effort to first assess what the cultural impacts and effects on Māori could be, and then consider whether and how to address those impacts and effects.

In general, this means we expect agencies to consider:

- Have you specifically consulted with Māori whose information you intend to collect to gather their views? Is it appropriate to do so in your circumstances? 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 governance, oversight or audit of your biometric system? Will you have representation from the people whose biometric information you are collecting?
- How can you mitigate or avoid any cultural impacts or harm that you identified?

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 to consider when assessing whether your use of biometric information is consistent with tikanga are:

- Ensuring that an individual’s mana, mauri and tapu is respected throughout the collection, use and disposal of biometric information.
- Considering Māori privacy from a collective, rather than solely individual, perspective.

- Ensuring that biometric data of living individuals is not stored with biometric data of deceased individuals.
- Ensuring Māori biometric information remains in New Zealand.
- Consideration of the concepts of utu (reciprocation) and ea (resolution or balance) in addressing any privacy breaches.

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 “more resources” section has links to other guidance which could assist you.

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. That does not make the processing disproportionate, but it is a factor to be considered.

On the other hand, strong negative impacts or effects which are not addressed could make the biometric processing disproportionate. The proportionality assessment is an overall assessment of the proportionality based on the risk, benefit and cultural impacts on Māori weighed together.

More 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, particularly the *Māori data sovereignty and privacy* discussion paper, 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
- Te Kāhui Raraunga- Māori Data Governance Model report by Te Mana Raraunga Māori Data Sovereignty Network, 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://www.tearawhiti.govt.nz/assets/Tools-and-Resources/Guidelines-for-engagement-with-Maori.pdf
- Crown engagement with Māori guidance from Te Arawhiti – the Office for Māori Crown Relations, available at: https://www.tearawhiti.govt.nz/tools-and-resources/crown-engagement-with-maori/
- 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).

Privacy safeguards

Rule 1 also requires you to put in place appropriate privacy safeguards before collecting information. If a privacy safeguard is relevant and reasonably practical for you to adopt or 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.

What makes a safeguard reasonable to implement?

When assessing whether a safeguard is relevant and reasonably practical to implement, you should consider:

- The kind of biometric system you will use.
- The complexity of your use of biometrics.
- The consequences for individuals if their biometric information is lost, misused, inappropriately accessed or disclosed etc.
- The consequences for individuals if there are errors in the biometric system.
- The ease and practicality of implementing the safeguard.
- The cost of implementing the safeguard.

A safeguard can still be reasonably practicable 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 reasonably practical.

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

The individual authorises the biometric processing and/or the individual can use an alternative to biometric processing

Giving individuals the choice to authorise the biometric processing or use an alternative to biometric processing is an important safeguard to mitigate privacy risk.

If you are implementing this 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.
- 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 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.

Authorisation must be explicit. You cannot rely on assumed 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 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 the authorisation safeguard.

Safeguards for if you are operating a biometric watchlist

A watchlist is where you have 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 for you to be operating a watchlist.

If you are operating a biometric watchlist, in general you should inform an individual on the watchlist:

- 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 delete the biometric information of anyone who is not one of those individuals, as soon as it is determined they are not on the watchlist.

If it is not safe to approach the individual or informing the individual would undermine the purpose of the biometric watchlist, then this safeguard will not be reasonably practical to implement in your circumstances. However, you should still consider whether you can provide general information about the watchlist e.g. on your website.

Examples:

- A clothing store is using FRT to identify individuals on a watchlist. Individuals are enrolled on the watchlist if they are trespassed from the site. 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. 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 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.

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.

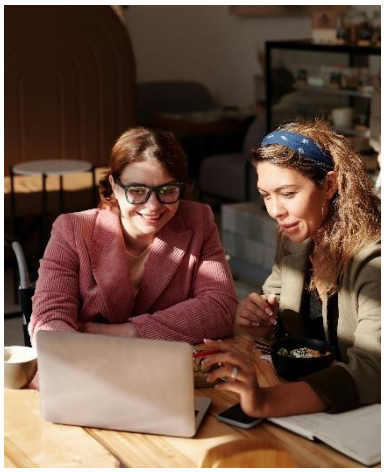
Protect biometric information with security safeguards

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 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 in connection with the provision of a service to an agency, ensure that the person has 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 general guidance on IPP 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.

In particular, 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.

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.

While 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 Biometrics 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.

Rule 1 Example Scenarios

Note: All the examples in the guidance are simplified and are for illustrative purposes only. They are not an endorsement or approval of any particular biometric system or 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 for access to an apartment building – Necessary and Proportionate

A body corporate for an apartment building wants to implement FRT as an alternative to swipe cards/keys for access for building residents.

Lawful purpose: To provide a secure form of access to the building for residents who choose to use the FRT system.

Initial plan for how the system will operate: a camera will be mounted on the exterior wall by the entrance door. The camera will activate when someone stands within a specific zone. At that point, the camera will scan the face of the person presenting to the camera. If there is a match between a person trying to enter the

building, and a person stored within the database, the door will unlock without the need of a key or a swipe card. Match information (whether a positive or a negative) will be deleted as soon as it is confirmed whether there is a match.

The body corporate consults with all residents of the building before the FRT is deployed and only continues with majority support. Because there will still need to be an access system for guests, building repair or maintenance personnel and emergency services (who will not be in the FRT database), the body corporate decides it will offer residents the choice to opt-in to FRT, or continue to use an alternative form of entry (such as key, swipe card or pin code).

Is the biometric processing necessary for the lawful purpose?

The body corporate determines the biometric processing is necessary for its lawful purpose because the biometric processing will be effective in achieving the lawful purpose and there is no alternative with less privacy risk.

Effectiveness: The body corporate assesses that the processing will be effective based on:

- Performance metrics from the provider of the biometric system.
- Information about the training or evaluation data that the provider used, compared with the residents of the building.
- Case studies of the use of FRT to regulate access to a building.
- Consultation with the residents of the building showing a general desire for and acceptance of the use of FRT.

Alternative means: There are alternative forms of biometric-based access to sites – for example, retina or fingerprint scans. These biometric alternatives have slightly different privacy risks, but overall are relatively consistent with FRT in this situation in terms of risk.

There are alternative ways to restrict access to the building (e.g. swipe card, key), but these would not provide the same benefit of a contactless, convenient form of access to the building. Instead, these alternatives will be offered to residents who

choose not to use FRT, and to those who need access but are not enrolled in the FRT database.

Is the biometric processing proportionate?

The body corporate believes that the biometric processing is proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- The positioning of the camera and how it will operate ensures the collection of biometric information is fairly targeted and reduces (but does not completely eliminate) the amount of information collected from individuals who have not authorised the collection/opted-in to the FRT system. So, there is some risk of capturing information of members of the public as well as residents. (In contrast, if the system was designed with a camera operating 24/7 that collected images of residents and members of the public walking past the building, this would substantially increase the risk).
- Individuals may suffer significant negative consequence by being denied access to their place of residence if there are issues e.g. misidentification through false negatives. False positives can also present a security risk.
- There will be a consultation and a clear authorisation/opt-in process which gives people genuine choice as to whether to use the system.
- Small risk that the use of FRT could result in some residents being deterred from exercising their freedom of movement e.g. if a resident who chose not to opt-in was still concerned about being seen by the camera so did not feel as free to enter and exit the building. Members of the public walking past may also be concerned, but the amount of information captured of non-residents will be very low and immediately deleted.
- Immediate deletion of match information reduces the amount of information stored.

- Some security risk from the stored biometric templates of residents using the FRT system.

Outcome of risk assessment: overall medium risk. The targeted scope of information being collected, consultation with and explicit authorisation from individuals, and immediate deletion of match information lowers the risk, but the consequences to individuals from misidentification, the small risk of deterring people from exercising protected rights, and security risk of stored information increases the risk. Implementing appropriate safeguards may be able to decrease the risk further (detailed further below).

Benefit: The benefit is increased convenience for the residents who choose to opt-in who will be able to enter the building in a contactless manner. This is a clear benefit to the individuals and carries a low to medium weight when weighed against the risk. Evidence (e.g. through consultation) that the increased convenience was particularly sought after and the FRT system was widely accepted by the residents could increase the weight of the benefit closer to the medium rather than low end of the scale. The body corporate considers the clear benefit to the individuals is sufficient to outweigh the privacy risk.

Cultural impacts on Māori:

- The body corporate consulted with all residents on the plan and sought specific feedback from Māori residents about their concerns.
- The main concern raised was the possibility of lower accuracy for Māori residents, which could lead to a higher rate of Māori residents being incorrectly denied access. The body corporate plans to mitigate this impact by ensuring the FRT is accurate across all demographic groups and actively monitoring the issue once the system is in place.

Overall proportionality assessment: Overall, the body corporate considers the biometric processing is proportionate:

Risk	Benefit	Cultural impacts
Medium risk use case.	Increase in convenience for residents who choose to use FRT.	Possibility of negative cultural impacts through potentially lower accuracy rates, but there is a plan to mitigate that impact.

Safeguards:

Some of the safeguards which are relevant and could help reduce privacy risk are:

- Clear authorisation from individuals sought and a non-biometric alternative provided.
- Thorough testing of the FRT system before deployment to assess different match thresholds.
- Deleting match information (non-match and match) once access is granted or denied.
- Processing residents' biometric samples into biometric templates and deleting the original samples.
- Using best practice security measures to protect the stored biometric templates.
- If an individual is denied access incorrectly, and they did not have a key or swipe, having a phone number to call to gain access with sufficient alternative identification.

Facial recognition at school for payment in a 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.

Lawful purpose: The lawful purpose is to manage the cafeteria queue efficiently and reduce the need for children to carry cash or a card to pay for food.

Initial plan for how the system will operate: The school will install cameras in the school cafeteria where children will be able to take food as desired and the facial recognition system will be used to identify the child and create an invoice for the food to send to the parents or caregivers for payment. Parents and caregivers will be able to choose whether their child can use the facial recognition system for payment. Images of children whose parents or caregivers did not give consent will be immediately deleted.

Is the biometric processing necessary for the lawful purpose?

After assessing the effectiveness and alternatives, the school is not confident that the biometric processing is necessary for the lawful purpose.

Effectiveness: After assessing the data from the FRT provider and considering a case study in the setting of a workplace cafeteria, it is not clear that the use of FRT will meaningfully reduce wait times. However, it could be an effective way to offer a cash/card free payment method.

Alternative means: There are alternative ways of meeting the lawful purpose of decreasing wait times, for example by adding an extra staff member. This would be significantly less privacy intrusive and likely more effective. There are also alternative ways of reducing the need to carry cash or a card to pay for food (e.g. through tokens or pre-payment of food), but these alternatives do have some downsides.

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.

Is the biometric processing proportionate?

The biometric processing would not be proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- Children are a more vulnerable population. Depending on the age and ability of each child, it may not be appropriate to rely on parental consent, and so relying on authorisation is not sufficient to mitigate the privacy risk.
- Authorisation is also not sufficient if all people who enter the cafeteria have their biometric information collected, whether or not they have authorised it.
- There is a risk of misidentification which could lead to financial consequences for individuals (incorrect billing of food items).
- Children may be more reluctant to use the school cafeteria because of monitoring by cameras and the reporting of their food purchases to their parents.

Outcome of risk assessment: overall high risk based on the fact children are a vulnerable population and there is no effective way to opt-out of a system that monitors the whole cafeteria, even if the food and payment details are only recorded for those who have authorised it.

Benefit: Increased convenience for students who will not have to carry cash or a card to purchase food. This benefit carries a low weight. If the biometric processing was effective at reducing wait times this would also offer a convenience benefit to the students and the school, but this would also carry a low weight.

Cultural 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 mokopuna.

Overall proportionality assessment: Overall, the biometric processing is **not** proportionate. There would need to be a very high level of benefit to justify the high privacy risk.

RISK	BENEFIT	CULTURAL IMPACTS
High risk use case. Authorisation is not a reliable way to mitigate risk when relying on parental consent, particularly for older children. In addition, biometric information may still be collected of children whose parents did not authorise the collection, meaning that authorisation is not an effective safeguard to reduce the risk.	Increased convenience (low weight).	Need to address tikanga of collecting information of mokopuna.

Safeguards: Even with safeguards like immediately deleting captured images once payment details were recorded, or governance/oversight of the biometric system, the risk would not be sufficiently mitigated to be proportionate, nor would the biometric processing be necessary.

Fingerprint scan to access secure information – Necessary and proportionate

Employer fingerprint for Multi Factor Authentication (MFA)

An employer has highly sensitive information that a limited number of employees have access to. Currently employees have access via password and an authenticator on a mobile device. Because of the highly sensitive nature of the information, the employer plans to use fingerprint access in place of the mobile authenticator.

Lawful purpose: To provide a high level of security protection for sensitive information.

Initial plan: the employer will undertake a consultation period about the need for increased security and plan to implement fingerprint MFA. If it decides to go ahead with fingerprint MFA, then employees will be required to provide a fingerprint sample and scan their fingerprint on a device at their desk to have access to the sensitive 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 if the employee requires access to the sensitive information.

Fingerprint templates will be stored locally on each device and will not be accessible by other employees or the employer management.

Is the biometric processing necessary for the lawful purpose?

The employer believes the biometric processing is necessary for its lawful purpose because the biometric processing will be effective in increasing the security protection and there is no alternative with less privacy risk.

Effectiveness: the employer believes the processing will be effective based on:

- Performance metrics from the provider of the biometric system.
- Evidence about the scientific or technical validity of overall process to address the issue/problem.
- Review of comparable uses domestically and in overseas jurisdictions.

Alternative means: There are various alternative forms of MFA that the employer could use, including both alternative biometric-based MFA and non-biometric based MFA. The employer considers the sensitivity of the information being protected justifies the use of a biometric-based MFA. In the employer's specific context, fingerprint-based MFA is the most practical compared with other forms of biometric-based MFA that could be used (such as iris scanning or FRT). This means that overall there is no alternative with less privacy risk.

Is the biometric processing proportionate?

The employer believes that the biometric processing is proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- Highly targeted security measure. Only fingerprint data from those who need to access the sensitive information will be collected.
- 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. Consulting with employees and offering the choice to opt-out (albeit with the consequence of losing access to the information and possible redeployment) provides some degree of mitigation against the power imbalance.
- Can use good security practices to protect the biometric information. This includes storing the fingerprint template locally on each device and ensuring access to the fingerprint template is restricted.

Outcome of risk assessment: Overall low to medium risk. The limited collection of biometric information and the security practices to protect it reduces the risk, but the context of the employment relationship increases the risk.

Benefit: Increase in level of security protection for sensitive information. This would likely carry a medium to high weight, depending on both how sensitive the information is, and the relative increase in security by using fingerprint scanning when compared with other forms of MFA.

Cultural 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 biometric system used has a high accuracy rating that does not differ among demographic groups.
- The fingerprints will be stored locally on each individual's device so no biometric information will leave New Zealand (better reflects Māori data sovereignty principles).

Overall proportionality assessment: Overall, the employer considers the biometric processing is proportionate:

Risk	Benefit	Cultural impacts
Medium risk use case.	Increase in security/protection of information (medium to high weight, depending on how sensitive the information in the database is and the relative increase in protection).	Consultation with Māori employees. Low risk of differing accuracy rates. Data stored in New Zealand.

Safeguards:

Some of the safeguards which are relevant and could help reduce privacy risk are:

- 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.

Voice sample and behavioural biometrics – Necessary and proportionate

A bank plans to use a range of biometric information for fraud detection and prevention purposes.

Lawful purpose: fraud prevention and detection.

Initial plan for how the system will operate: The bank will collect a voice sample from customers 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 (biometric characteristic). This information will be used to create a customer profile and generate an alert if there is a noticeable change in voice or behaviour that could indicate fraud.

Is the biometric processing necessary for the lawful purpose?

The bank assesses that the biometric processing is necessary for its lawful purpose because the biometric processing will be effective in achieving the lawful purpose and there is no alternative with less privacy risk.

Effectiveness: The bank determined the processing will be effective based on:

- Performance metrics from the provider of the biometric system.
- Evidence about the scientific or technical validity of overall process to address the issue/problem.
- Academic/scientific research.
- Review of comparable use domestically or in overseas jurisdiction

Alternative means: The bank considers there is no real non-biometrics alternative that would offer a similar ability to achieve the bank's lawful purpose.

Is the biometric processing proportionate?

The bank assesses that the biometric processing is proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- Some degree of power imbalance but overall context and purpose of collection (fraud detection/prevention) lowers impact of the power imbalance.
- Low risk of impact on protected rights.
- It will not be possible to opt-out (because that would be detrimental to the purpose of preventing fraud), which means individuals have less choice about how their information is collected and used.
- Could be accuracy issues with the creation of customer profile based on behavioural biometric information.

Outcome of risk assessment: overall low risk based on type of information collected, type of relationship between bank and customer and impact on protected rights.

Benefit: increase in security and reduction in fraud. Medium to high weight, depending on how strong the evidence is for a reduction in fraud.

Cultural impacts on Māori:

- The bank plans to design the system in a way that would not distinguish between Māori and non-Māori information – i.e. not linked with any ethnicity or cultural information.
- Will have a governance board of biometrics system with Māori representation.

Overall proportionality assessment: Overall, bank considers the biometric processing is proportionate:

Risk	Benefit	Cultural impacts
Low risk use case. Low risk design of system.	Expected to increase security and help prevent and detect fraud (medium to high weight).	Low risk of negative cultural impacts Will have Māori representation on governance board.

Safeguards:

Some of the safeguards which are relevant and could help reduce privacy risk are:

- Good transparency with bank customers about what information is collected.
- Thorough testing of the system before deployment.
- Using best practice security measures to protect the biometric information.