Privacy Commissioner
Te Mana Mātāpono Matatapu

# Biometric Processing Privacy Code draft guide – appendix: applying the Code to example use cases

Privacy Commissioner
Te Mana Mātāpono Matatapu

# Biometrics guidance appendix: Applying the Code to example use cases

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

> A note on OPC's examples: All the examples in the guidance are simplified and are for illustrative purposes only. They do not represent an endorsement or approval of any particular type of biometrics 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.

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

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

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

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

BIC will be Novel Investments' agent and will not use or disclose the information for its own purposes. Therefore, Novel Investments is responsible under the Privacy Act and needs to check if Novel Investments can comply with the biometric processing Code. See our guidance on using third party providers for more information.

| Rule | How the code could apply |
|---|---|
| Does the Code apply? | Yes, Novel Investments will collect and use biometric information for biometric verification (facial images used in facial recognition technology). |
| Rule 1 – Purpose for collection | Novel Investments' **lawful purpose** is to comply with a legal obligation to verify customer identities.<br><br>Novel Investments determines that biometric processing is **necessary** for that lawful purpose. In particular:<br><br>• **Effectiveness**: There is a clear link between the biometric processing and Novel Investments' lawful purpose. Novel Investments obtained evidence such as statistics and test performance data from BIC that gives Novel Investments confidence that the biometric processing will be effective in accurately verifying customer identities.<br>• **Alternative**: Novel Investments researched different options for verifying customer identities remotely. They are satisfied that there is no other sufficiently robust way to meet the obligation to verify the identity of new customers who are accessing their services remotely. However, manual verification will be provided as an alternative option where a new customer has difficulty using BIC's service or is sensitive about the processing of their biometric information. Manual verification will require |

| Rule | How the code could apply |
|---|---|
| | customers to travel to one of Novel Investments' offices in person.<br><br>Novel Investments determines that the biometric processing is **proportionate** because:<br><br>• Novel Investments assesses the **privacy risk** as low based on:<br>  ○ Highly accurate system with limited, targeted collection. The live selfie will be deleted as soon as identity is verified.<br>  ○ Individual authorisation will be sought and a manual, in-person alternative will be available.<br>  ○ Low risk of bias, low risk of chilling effect on protected rights.<br>  ○ Implementation of privacy safeguards detailed further below.<br>• Novel Investments considers there is a medium to high **benefit** that outweighs the privacy risk based on:<br>  ○ There is a clear benefit to individuals who will be able to verify their identities remotely.<br>  ○ The benefit to Novel Investments of a more robust, convenient and cost-effective way of verifying customer identities substantially outweighs the low privacy risk.<br>• Novel Investments considers **cultural impacts** on Māori:<br>  ○ Novel Investments confirms BIC's accuracy rates for Māori are equivalent to non-Māori. |

| Rule | How the code could apply |
|---|---|
| | ○ Individual authorisation will be sought to mitigate potential cultural impacts and an alternative to biometric processing will be available.<br>○ Novel Investments chose BIC over another provider because BIC stores the biometric information collected on cloud storage in New Zealand, and this option better reflects the principles of Māori data sovereignty.<br>• **Overall proportionality**: The biometric processing is proportionate due to minimal privacy risk/impact, strong benefits to the customers and business and the mitigation of impacts/effects on Māori customers.<br><br>Novel Investments will adopt reasonable **privacy safeguards**, including:<br>• Obtaining individual authorisation and providing an alternative to biometric processing.<br>• Having sufficient assurances (e.g. through contract obligations) that BIC uses best practice security safeguards.<br>• Monitoring accuracy rates.<br>• Deleting the live selfie as soon as the customer's identity is verified.<br>• Liveness check to prevent spoofing |

| Rule | How the code could apply |
|---|---|
| Rule 2 – source of biometric information | Novel Investments is collecting biometric information directly from the individual. Even though Novel Investments is engaging a third-party provider, because BIC is acting as Novel Investments' agent, this is still considered direct collection. |
| Rule 3 – collection of information from individual | Novel Investments will meet the rule 3 requirements when the customer first signs up, using a plain language, clear and accessible written statement that is included as part of the customer application. |
| Rule 4 – manner of collection | Novel Investments is collecting information by lawful means. It ensures its manner of collection is fair and not unreasonably intrusive, including when customers may be vulnerable or children or young people. If Novel Investments has any customers who are children or young people, it will offer manual processing as a first choice or allow biometric processing with parental/caregiver authorisation.<br><br>Seeking individual authorisation and offering an alternative to biometric processing is one of the ways Novel Investments ensures the manner of collection is lawful, fair and not unreasonably intrusive. |

| Rule | How the code could apply |
|---|---|
| Rule 5 – Storage and security of biometric information | Novel Investments chose BIC because BIC uses best practice security safeguards. Novel Investments also ensures that it has contractual mechanisms in place to give it confidence that the storage and security practices of BIC meet Novel Investments' requirements. Novel Investments conducts regular audits and assurance checks to confirm the security safeguards used by BIC remain appropriate.<br><br>See our Security and Access controls guidance in Poupou Matatapu for more information on storage and security of information. |
| Rule 6: Access to biometric information | Novel Investments will comply with requests to access biometric information.<br><br>It will confirm if it holds any biometric information about an individual. Because the live selfie will be deleted as soon as the customer's identity is verified, in general Novel Investments will confirm that it holds a copy of the individual's identity document (if this is still held) and a record of the fact that the customer's identity was verified through biometric verification. |

| Rule | How the code could apply |
|---|---|
| Rule 7: Correction of biometric information | Novel Investments will comply with requests to correct biometric information. Because the live selfie will be deleted as soon as the customer's identity is verified, in general the only biometric information available to be corrected will be a result and the copy of the individual's identity document (if this is still held). Novel Investments ensures that its arrangement with BIC will allow it to access and correct information in a timely manner, including the ability to add a statement of correction from a customer. Novel Investments can also seek details if required from BIC about the accuracy of any match result. |
| Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure | Novel Investments has researched the accuracy of BIC's matching process and determined it is acceptable for Novel Investments' purposes. However, errors may still occur so Novel Investments ensures there are ways for customers to address errors if their identity verification is inaccurately rejected. |
| Rule 9: Retention of biometric information | The live selfie will be deleted as soon as the identity is verified. Other biometric information will only be retained for as long as required to comply with Novel Investments' legal obligation to verify customer identities. |

| Rule | How the code could apply |
|---|---|
| Rule 10: Limits on use of information | Novel Investments' use of biometric information would not be restricted by the fair use limits because it is not using the facial image data to collect/infer health data, emotion data, or categorise the individual according to a demographic category protected by the Human Rights Act.<br><br>Novel Investments ensures it only uses the biometric information for the purpose of verifying customer identities and no other purpose, because it is unlikely another exception in rule 10 would apply. |
| Rule 11: Limits on disclosure of biometric information | Novel Investments will not disclose the biometric information. |
| Rule 12: Disclosure of biometric information outside New Zealand | Novel Investments will not disclose information outside New Zealand. |
| Rule 13: Unique identifiers | Novel Investments will not assign a biometric feature or biometric template to customers as a unique identifier. |

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

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

| Rule | How the code could apply |
|---|---|
| Does the Code apply? | Yes, SIL is collecting fingerprints (biometric information) to use in biometric verification. |
| Rule 1 – Purpose for collection | SIL's **lawful purpose** is to protect highly sensitive personal information. Organisations are required under the Privacy Act to protect personal information using reasonable security safeguards.<br><br>SIL determines that the biometric processing is **necessary** for that lawful purpose. In particular:<br>• **Effectiveness**: There is a clear link between the biometric processing and SIL's lawful purpose. MFA is a widely used way to protect personal information, and there is an evidential basis that fingerprint scanning offers a highly effective form of protection. SIL confirms the effectiveness of the specific MFA system they intend to use, as well as considering effectiveness of fingerprint scanning for MFA more generally.<br>• **Alternative**: SIL researched different MFA options and the differing levels of security each provides. SIL is satisfied that the sensitivity of the information they need to protect requires a form of MFA with |

| Rule | How the code could apply |
|---|---|
| | particularly high security and low chance of spoofing. Therefore SIL is satisfied that they cannot achieve the same level of protection without using biometric processing.<br><br>SIL determines that the biometric processing is **proportionate** because:<br>• SIL assesses the **privacy risk** as low to medium based on:<br>  ○ The MFA measure is targeted so fingerprint data will be collected only from those who need to access the sensitive information.<br>  ○ The context of the employment relationship increases the intrusiveness of the measure as the power imbalance may mean employees feel coerced into giving their biometric data. To help mitigate this risk, SIL will consult with employees on whether it is practical to allow employees to opt-out of giving their biometric information (but in that case the employee would lose access to the sensitive information and may require changes to their job following the normal employment process).<br>• SIL considers there is a medium to high **benefit** that outweighs the privacy risk based on:<br>  ○ SIL having a highly effective security measure in place that protects sensitive information and reduces the risk of privacy breaches. It also benefits the individuals whose sensitive personal information is |

| Rule | How the code could apply |
|---|---|
| | being protected. This benefit substantially outweighs the low to medium privacy risk.<br>• SIL considers **cultural impacts** on Māori:<br>  ○ As part of SIL's consultation with employees, it will specifically seek feedback on cultural impacts from Māori employees and consider how to address any impacts raised.<br>  ○ The biometric system used has a high accuracy rating regardless of skin tone.<br>  ○ The fingerprints will be stored locally on each individual's device so no biometric information will leave New Zealand.<br>• **Overall proportionality:** Despite some level of intrusiveness, overall the measure is proportionate due to the heightened need for robust security measures to protect the sensitive personal information. The privacy and employment impact on employees can be further mitigated by safeguards (see below).<br><br>SIL will adopt reasonable **privacy safeguards**, including:<br>• SIL will consult with employees before introducing the system and offer the ability to opt-out of providing biometric information (but then the employee would lose access to the sensitive information). If the consultation reveals significant employee concerns, the organisation will work with employees to resolve or mitigate the concerns before continuing with the fingerprint MFA system. |

| Rule | How the code could apply |
|---|---|
| | • SIL will only retain a template of the fingerprint scan, not the actual scan, to reduce risks of spoofing and presentation attacks.<br>• SIL will use best practice security measures to protect the biometric information, including having a process in place to audit any access to the fingerprint templates to identify any employee browsing issues.<br>• Not linking the fingerprint information with any other personal information of the employee. |
| Rule 2 – source of biometric information | SIL is collecting biometric information directly from the individual. |
| Rule 3 – collection of information from individual | SIL will comply with rule 3 by informing the employees of the purpose of collection, alternative option and consequences for not providing a fingerprint etc. as part of the consultation before using the system. It will also give employees a plain language, written statement at the time that they provide a fingerprint sample and add information to the employee intranet. |
| Rule 4 – manner of collection | SIL is collecting information by lawful means. It will not collect any biometric information of children or young people. Consulting with employees and offering an opt-out of biometric processing is one of the ways SIL ensures the manner of collection is lawful, fair and not unreasonably intrusive. |

| Rule | How the code could apply |
|---|---|
| Rule 5 – Storage and security of biometric information | SIL is using biometric information to protect other personal information. But it still needs to ensure the biometric information is appropriately protected.<br><br>Some ways SIL decides to protect the employee fingerprint information is by:<br>• Deleting the original samples and only storing the biometric template.<br>• Storing the template locally on the device.<br>• Not linking the fingerprint template with any other personal information of the employee. |
| Rule 6: Access to biometric information | SIL will comply with requests to access biometric information.<br><br>Because the fingerprint sample will be deleted as soon as the employee's fingerprint template is generated, in general SIL will confirm that it holds a template about the individual. The templates may not be extractable to provide to the employee, so in that case SIL will provide an explanation that it holds a template and what that means. |

| Rule | How the code could apply |
|---|---|
| Rule 7: Correction of biometric information | SIL will comply with requests to correct biometric information.<br><br>Because the fingerprint sample will be deleted as soon as the employee's fingerprint template is generated, and the templates may not be extractable to provide to the employee, in general there will not be any biometric information that the employee will be able to correct. However, SIL decides that if an employee has a concern and wishes to correct their biometric information, it will delete the stored template and re-enrol the employee in the system. |
| Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure | The way in which biometric information is being collected and used by SIL is unlikely to raise issues under rule 8. Collecting the fingerprint samples directly from the employees helps ensure the information is accurate before it is used. SIL will have processes in place to update the information if needed, e.g. if an employee injured their finger resulting in a changed fingerprint. |
| Rule 9: Retention of biometric information | SIL will only store the fingerprint template for as long as an employee requires access to the sensitive information.<br><br>If an employee goes on extended leave, SIL will consider whether to delete the employee's fingerprint template and re-enrol them when they return. |

| Rule | How the code could apply |
|---|---|
| Rule 10: Limits on use of information | SIL's use of biometric information would not be restricted by the fair use limits because it is not using the fingerprint to collect/infer health data, emotion data, or categorise the individual according to a demographic category protected by the Human Rights Act.<br><br>SIL will ensure it only uses the biometric information for the purpose of MFA and no other purpose, because it is unlikely another exception in rule 10 would apply. |
| Rule 11: Limits on disclosure of biometric information | SIL will not disclose the biometric information. |
| Rule 12: Disclosure of biometric information outside New Zealand | SIL will not disclose information outside New Zealand. |
| Rule 13: Unique identifiers | SIL will not assign a biometric feature or biometric template to customers as a unique identifier. |

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

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

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

| Rule | How the code could apply |
|---|---|
| Does the Code apply? | Yes, Busy Machinery is collecting facial images (biometric information) to identify people (biometric identification). |
| Rule 1 – Purpose for collection | Busy Machinery's **lawful purpose** is to put in place a more robust process to keep workers safe and comply with legal health and safety requirements.<br><br>Busy Machinery determines that the biometric processing is **necessary** for that lawful purpose. In particular:<br>• **Effectiveness**: There is a clear link between the biometric processing and Busy Machinery's lawful purpose. The FRT provider Busy Machinery chose |

| Rule | How the code could apply |
|---|---|
| | has deployed this type of solution in similarly dangerous work environments before and has data showing how it worked, how it can help in the event of a health and safety incident, as well as a reduction in unauthorised access to restricted areas. The facial recognition algorithm chosen has a high accuracy rating across demographics and could be set to an appropriate specificity and sensitivity level that balanced false negatives (disrupting workflows) and false positives (guarding against unauthorised people).<br>• **Alternative**: There are other ways for Busy Machinery to monitor workers on site and control access but these all had significant drawbacks. It was important for Busy Machinery to find a seamless 'contactless' way of monitoring each worker entering and exiting. Busy Machinery considered a physical access card option or sign on in a paper register at the site entrance. Workers are usually wearing physical protective suits and/or carrying equipment that would make using these alternatives more difficult and less convenient. Cards can also be passed from an authorised user to an unauthorised user, creating safety risks.<br><br>Busy Machinery considers the proportionality of the measure:<br>• Busy Machinery assesses the **privacy risk** as medium to high based on:<br>o Monitoring a workspace using FRT that records live attendance onsite poses a |

| Rule | How the code could apply |
|---|---|
| | medium to high level of intrusiveness, more than the use of CCTV because FRT will identify individuals.<br>○ 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.<br>○ There is some risk of scope creep as information collected for safety purposes could be useful for other employment purposes (monitoring performance, time management, disciplinary actions).<br>○ Everyone who enters the worksite will be affected, including those who accidentally enter. There will not be an opt-out/alternative set up because it would undermine the integrity of the system.<br>○ There is a possibility of false negatives which could be disruptive/alarming for a worker who is authorised – they would have to challenge automated decision. Busy Machinery will need to have human oversight of any automated alerts so there can be a human review before any action is taken.<br>○ Counting the number of persons present on site (so there was a live log of this in case of an incident) is less invasive than monitoring identifiable individuals (even though the system counts by recognising unique faces).<br>• Busy Machinery considers there is a medium to high **benefit** that outweighs the privacy risk based on: |

| Rule | How the code could apply |
|---|---|
| | ○ There is a clear benefit to the individuals from improved health and safety and convenience from not having to present a physical access card or sign in at the site entrance.<br>○ There is a benefit to Busy Machinery from improved management of health and safety risks and a reduction in unauthorised access to restricted areas.<br>• Busy Machinery considers **cultural impacts** on Māori:<br>○ Some workers are Māori and wear moko, so there is culturally sensitive/tapu information that will be captured by the FRT system (even though the FRT system will not be analysing the moko specifically).<br>○ The FRT system will not be optional and there will be no opt-out, which could raise tikanga issues around obtaining free, prior informed consent and giving people control over their own information.<br>• **Overall proportionality:** based on the initial assessment, Busy Machinery was not confident that the measure was proportionate, given the medium to high privacy risk, cultural impacts on Māori and possible discriminatory effects. However, because Busy Machinery thought the FRT was a better solution than the alternatives considered, they considered additional safeguards to lower the overall risk/intrusiveness of the proposal, and therefore make the measure proportionate. |

| Rule | How the code could apply |
|---|---|
| | Busy Machinery will adopt reasonable **privacy safeguards**, including:<br>• There will be a strict policy around access to and use of data, backed up with robust access and audit controls. Information from the FRT system will only be used for health and safety and incident responses, not performance, disciplinary actions, or covertly watching employees.<br>• The daily log of data collected will be deleted as soon as the site manager confirms that there was no health and safety incident.<br>• Busy Machinery consulted with workers about the FRT system as well as the other non-biometric options. The outcome of the consultation was that the workers were comfortable with the FRT system as long as above safeguards adopted.<br>• The system will be regularly reviewed to ensure it is sufficiently effective and information is adequately protected.<br><br>After considering how the safeguards impact the overall risk of the system, Busy Machinery is comfortable that the risk is medium rather than high and that the benefit is sufficient to make the system proportionate overall. |
| Rule 2 – source of biometric information | Biometric information (facial image/scan) is collected directly from the workers to enrol them in the database and each time they enter the worksite. Remote collection (e.g. by a FRT camera) is still considered direct collection for the purposes of rule 2. |

| Rule | How the code could apply |
|---|---|
| Rule 3 – collection of information from individual | Busy Machinery will comply with rule 3 by informing the workers of the purpose of collection, no alternative option etc. as part of the consultation before using the system. It will also give workers a plain language written statement at the time that they enrol in the system.<br><br>A sign will also be installed at the entrance to the site so that anyone new to site also receives the information required by rule 3. |
| Rule 4 – manner of collection | Busy Machinery is collecting information by lawful means. It does not expect to collect any biometric information of children or young people.<br><br>Consulting with workers and ensuring good transparency around when and how the biometric information is collected is one of the ways Busy Machinery ensures the manner of collection is lawful, fair and not unreasonably intrusive. It will also ensure cameras are not stationed at any areas where sensitive information, or information that is not necessary for the purpose, would be collected – for example, no cameras in or pointing at the break room or bathrooms. |

| Rule | How the code could apply |
|---|---|
| Rule 5 – Storage and security of biometric information | Some ways Busy Machinery decides to protect the biometric information is by:<br>• Robust access and audit controls for information collected through the FRT system.<br>• Deleting daily log of data once there is confirmation of no health and safety incident.<br>• Not linking information collected through the FRT system with any other personal information of workers. |
| Rule 6: Access to biometric information | Busy Machinery will comply with requests to access biometric information. |
| Rule 7: Correction of biometric information | Busy Machinery will comply with requests to correct biometric information.<br><br>Where appropriate, Busy Machinery will delete the stored template and re-enrol the worker in the system. |
| Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure | The way in which biometric information is being collected and used by Busy Machinery is unlikely to raise issues under rule 8. |
| Rule 9: Retention of biometric information | Busy Machinery will delete the daily log of data once there is confirmation of no health and safety incident.<br><br>Biometric samples and templates will be deleted immediately once the relevant worker no longer requires access to the site. |

| Rule | How the code could apply |
|---|---|
| Rule 10: Limits on use of information | Busy Machinery's use of biometric information would not be restricted by the fair use limits because it is not using the fingerprint to collect/infer health data, emotion data, or categorise the individual according to a demographic category protected by the Human Rights Act. This could change if Busy Machinery was trying to collect or infer health data as part of the health and safety incident monitoring, depending on the level of risk to staff safety, and whether employees were expressly informed and authorised this.<br><br>Busy Machinery still needs to ensure it only uses the biometric information for its original lawful purpose and no other purpose, because it is unlikely another exception in rule 10 would apply. |
| Rule 11: Limits on disclosure of biometric information | Busy Machinery may need to disclose information about a health and safety incident to a regulatory body such as Work Safe. This would likely be permitted under the exception that allows disclosure for a directly related purpose. Busy Machinery includes this possibility in the information it gives workers under rule 3.<br><br>Busy Machinery does not intend to make any other disclosures. |
| Rule 12: Disclosure of biometric information outside New Zealand | Busy Machinery will not disclose information outside New Zealand. |
| Rule 13: Unique identifiers | Busy Machinery will not assign a biometric feature or biometric template to customers as a unique identifier. |