NZCTU
Te Kauae Kaimahi

Submission to the Office of the Privacy Commissioner on:

Biometric Processing Privacy Code Exposure Draft

Submitted by the New Zealand Council of Trade Unions Te Kauae Kaimahi

8 May 2024

This submission is made on behalf of the 31 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With over 340,000 union members, the CTU is one of the largest democratic organisations in New Zealand.

The CTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga), the Māori arm of Te Kauae Kaimahi (CTU), which represents approximately 60,000 Māori workers.

Contents

1. Summary of recommendations

1.1. The New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU) strongly supports the OPC's decision to issue a code of practice for biometric processing.

1.2. However, our view is that some aspects of the draft code are underpowered and will not sufficiently protect workers from the privacy risks associated with biometric processing.

1.3. The CTU recommends the following revisions to the draft code:

1.3.1. Rule 1: Biometric information should only be collected for a *reasonable, legitimate, and lawful purpose*. Currently, Rule 1(1) only requires that it be for a lawful purpose.

1.3.2. Rule 1: Agencies should be required to *establish*, on reasonable grounds, that biometric processing is not disproportionate in the circumstances. Currently, Rule 1(1) only requires that an agency must "believe" this.

1.3.3. Rule 1: Agencies should be required to *undertake and produce* a proportionality assessment. Currently, Rule 1(2) only requires that an agency must "take into account" various issues, and there is no requirement to produce a written record of this analysis that can be referred to.

1.3.4. Rule 1: Agencies should be required to *undertake and produce* a risk assessment. There is currently no such requirement in the draft code.

1.3.5. Rule 1: If biometric processing is to be used in the context of an employment relationship, agencies should be required to undertake the proportionality test and the risk assessment in consultation with workers and their representatives in trade unions.

1.3.6. Rule 1: Agencies should be required to ensure that all *necessary* privacy safeguards and security measures are in place, not just those that are considered "reasonably practicable".

1.3.7. Rule 1: Agencies should be required to assess *how privacy risks are distributed* – i.e., who bears the privacy risks associated with a type of biometric processing.

1.3.8. Rule 1: Agencies should only be able to collect biometric information from workers if the privacy risks to those workers are outweighed by the benefits to those same workers.

1.3.9. Rule 3: The conditions set out in Rule 3(1) should be mandatory if information is being collected in the context of an employment relationship. Currently, agencies are only required to take steps that are "in the circumstances reasonable".

1.3.10. Rule 3: Valid consent should be a mandatory requirement for collecting biometric information in the employment context. Currently, there is no mandatory consent requirement in the draft code.

1.3.11. Rule 3: To improve workers' ability to provide valid consent, an additional section should be added to Rule 3 requiring that an employer must not collect biometric information from a worker unless the worker has:

- Provided specific and express consent for each purpose of collection.
- Been provided with the opportunity to seek advice and comment on the lawfulness of the collection.
- Been sufficiently informed of the potential value of their biometric information, the known and potential risks associated with the collection and processing of their biometric information, and the actions that will be taken to safeguard their biometric information.
- Been provided with reasonable alternatives to the collection of their biometric information, without penalty or threat of penalty.

1.3.12. Rule 3: In the context of an employment relationship, the collection of biometric information should be restricted to the workplace and work hours.

1.3.13. Rule 10: Rule 10(3)(b)(i) increases the risk of scope creep and should be deleted.

1.3.14. Section 3: Heartbeat should be included in the definition of behavioural biometrics if this information is being collected in the employment context.

1.3.15. Section 3: The OPC should further analyse the risks associated with excluding "readily apparent expressions" from the definition of biometric classification.

1.3.16. The OPC should commission a study into the prevalence and types of biometric processing covered by the code that are occurring in New Zealand.

2. Introduction

2.1. The New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU) welcomes the opportunity to submit to the Office of the Privacy Commissioner on the Biometric Processing Privacy Code Exposure Draft ("the draft code").

2.2. In 2023, the CTU supported the OPC's proposal to issue a code of practice and provided a written submission on the kinds of safeguards we think are needed to ensure the responsible collection and processing of biometric data in the workplace.[1] A sufficiently robust code of practice will help workers and their representatives in trade unions to insist on their rights and to ensure their safety and the safety of others.

2.3. The use of biometric technologies in the workplace is becoming more common. Hoffman and Mariniello identify four main purposes that biometric technologies are used for in the workplace: (1) security; (2) recruitment; (3) monitoring/surveillance; and (4) health and safety.[2]

2.4. The academic and policy literature finds that, except for their use for health and safety purposes (which is not without risks), biometric technologies offer few benefits to workers and often generate significant privacy risks.[3] These risks include:

- **The misuse of workers' biometric information**. Given the highly personal and sensitive nature of biometric information, its collection generates risks such as the accidental disclosure to employers of information such as medical conditions, the improper use of biometric information by an employer, and security breaches of biometric information held by an employer or third party.
- **The use of biometrics to surveil and control workers**. Biometric wearables, concentration tracking software, and keystroke monitoring software are becoming more widely used in workplaces. Research finds that workplace surveillance technologies significantly increase job stress and tend to reduce job satisfaction.
- **Bias and discrimination in consequential management decisions**. Biometric information is used as an input in some automatic recruitment, performance

[1] NZCTU, "Submission to the OPC: Consultation on a Potential Code of Practice for Biometrics" (2023).
[2] M. Hoffman and M. Mariniello, "Biometric Technologies at Work: A Proposed Use-Based Taxonomy", *Bruegel Policy Contribution No 23/2021* (2021).
[3] For overviews, see: K. Ball, *Electronic Monitoring and Surveillance in the Workplace* (European Commission, 2021); P. Holland and T. L. Tham, "Workplace Biometrics: Protecting Employee Privacy One Fingerprint at a Time", *Economic and Industrial Democracy* 43 (2020); D. Ravid et al., "A Meta-Analysis of the Effects of Electronic Performance Monitoring on Work Outcomes", *Personal Psychology* 76 (2023); T. Kalischko and R. Riedl, "On the Consequences of Electronic Performance Monitoring in Organizations: Theory and Evidence", *Digital Transformation and Society* 3 (2024).

management, and day-to-day task management. Research has established that this can produce biased results and discriminatory outcomes.

- **Function and scope creep**. This occurs when workers' biometric information is collected or processed for a different purpose than originally intended. Because of the power imbalance in the employment relationship, workers are particularly vulnerable to function and scope creep. If not sufficiently regulated, there is a risk that workers' will be subjected to increasingly intrusive practices as the use of biometric technologies becomes normalised.

2.5. Perhaps the most famous example of how biometrics can be harmfully deployed in the workplace is in Amazon warehouses. There, workers are required to wear trackables that monitor their productivity and their "time off task", and which can send automatic dismissal notices to workers if they fail to meet algorithmically determined productivity targets.[4]

2.6. Although we are strongly supportive of a code of practice being issued, we think some aspects of the draft code are significantly underpowered and will not protect workers from these risks (and other risks identified in section 3(2) of the draft code).

2.7. Given the deeply personal and sensitive nature of biometric information, and the fundamental questions of human dignity and freedom that are raised by its collection in the employment context, our view is that:

- Employers should have to clear a very high bar if they are to collect and process workers' biometric information. This extends across the purpose and method of collection and processing, the storage and security practices, and the processes by which decisions relating to biometric information are made.
- Workers should be entitled to be properly engaged in any decision relating to the collection and processing of their biometric information.
- Individuals are the ultimate owners of any data about themselves and should be able to access the data that they produce and use it to protect and further their own interests.[5]

2.8. The remainder of the submission focuses on how the draft code applies to the employment context. We provide specific recommendations for how the code can be strengthened to better protect workers from the risks associated with biometric

[4] Center for Labor and a Just Economy at Harvard Law School, "Worker Power and Voice in the AI Response" (2024), pp. 6-7.
[5] See R. Allen and D. Masters, *Technology Managing People – The Legal Implications* (TUC, 2023), p. 95.

technology. Overall, we recommend significant revisions and extensions are made to Rule 1 and Rule 3. We provide specific revisions to the drafting of the code in the Appendix.

3. Purpose of collection and proportionality

3.1. We strongly support the requirement that agencies must conduct a proportionality test before collecting or processing biometric information.

3.2. However, as it is currently drafted Rule 1 does not set sufficient obligations upon agencies to conduct thorough and measured proportionality assessments. This increases the risk that biometric information will be unnecessarily or improperly collected in the employment context.

3.3. Rule 1(1)(a) requires that biometric information must only be collected for a lawful purpose. But there are many lawful purposes that are, in themselves, relatively trivial – for example, the purpose of "improving convenience" – or are vague – for example, the purpose of "supporting innovation". The risk of trivial or vague purposes being used to collect biometric information is somewhat mitigated by Rule 1(1)(d). However, given the sensitivity of biometric information, and the central questions of human dignity and freedom that are tied up with it, we recommend that, in addition to the requirement that biometric information must only be collected for a lawful purpose, it should also be for a *reasonable and legitimate* purpose.

3.4. Although Rule 1(1)(d) sets a proportionality condition that must be met if biometric information is to be collected, in determining whether the collection/processing of biometric information is proportionate an agency is only required to "take into account" a set of circumstances. For example, an agency is only required to "take into account whether or not biometric processing is effective in achieving the agency's lawful purpose" (Rule 1(2)(a)). This is a highly variable test to apply and increases the risk that the proportionality test will become a box-ticking compliance exercise, rather than a meaningful and considered analysis of the potential risks and benefits, and the balance between them. Additionally, the issues that must be taken into account are themselves quite a limited set. To address these issues, we recommend:

- Agencies should be required to *establish*, on reasonable grounds, that biometric processing is not disproportionate in the particular circumstances. At present, Rule 1(1)(d) only provides that an agency must "believe" this.

- Agencies should be required to *undertake and produce* a proportionality assessment. Rule 1(2) only provides that an agency must "take into account" various issues, and thus there is no requirement to produce a written record of this analysis that can be referred to.
- Agencies should be required to include in their proportionality assessment the following: a description of the proposed method of biometric processing; the date from which it will be implemented; the types of decisions it will be used to support; the proposed purpose of using the system; the logic which will underpin the system (e.g., any algorithms that are used); whether it will be effective in achieving its purpose; the degree of privacy risk and who carries these risks; whether the purpose can be achieved by alternative means; and any cultural impacts.
- If biometric processing is to be used in the context of an employment relationship, agencies should be required to undertake the proportionality test in consultation with workers and their representatives in trade unions.

4. Risk assessment

4.1. Overall, we do not think the draft code sets sufficiently rigorous obligations regarding the assessment of potential privacy risks and their management.

4.2. First, although agencies must "take into account [...] the degree of privacy risk from the type of biometric processing" they are considering using (Rule 1(2)), there is no requirement for thorough risk assessments to be conducted. Thus, while eight areas of privacy risk are identified in section 3(2) of the draft code, there is no process specified by which agencies are expected to measure the prevalence of these risks, to weigh the balance between the perceived risks and benefits, to assess how the perceived risks and benefits may be distributed among the actors involved, the kinds of privacy safeguards that would be necessary to employ, and the agency's capacity to put in place and maintain these safeguards, among other issues. This increases the risk of agencies deploying biometric technology without having undertaken thorough risk assessments or understanding the potential implications of using this technology.

4.3. To address this issue, we recommend:

- Agencies should be obliged to *undertake and produce* a risk assessment, which could be included within or be separate to the proportionality assessment. This risk assessment should cover the different privacy risks associated with the type of

biometric processing used, who is exposed to these risks, the likelihood of these risks occurring, the consequences of these risks occurring, the privacy safeguards that are necessary, and the agency's capacity to implement and maintain these privacy safeguards.[6]

- If biometric processing is to be used in the context of an employment relationship, agencies should be required to undertake the risk assessment in consultation with workers and their representatives in trade unions.

5. Privacy safeguards and security

5.1. Rule 1(1)(c) requires that agencies must adopt or implement "such privacy safeguards as are reasonable in the circumstances (if any)". The definition of "privacy safeguard" is defined in section 3(3) as "actions or processes that are relevant and reasonably practicable in the circumstances to reduce privacy risk". Rule 5 also sets out security and storage requirements that must be adopted.

5.2. Our view is that these provisions are underpowered. They do not place a sufficiently strong obligation on agencies to ensure that the *necessary* privacy safeguards and security measures are in place. For example, the current drafting of the code leaves open the possibility that an agency may identify a privacy safeguard as relevant or even necessary, but not reasonably practicable. This raises the risk that necessary safeguards will not be put in place because it is not practicable to do so (or an employer incorrectly judges that it is not practicable to do so).

5.3. To address this issue, we recommend the following changes to the language of the draft:

- Rule 1(1)(c): Revise from "reasonable" to "reasonable and necessary".
- Section 3(3): Revise the definition of privacy safeguard to replace "relevant and reasonably practicable" with "relevant and necessary".
- Rule 5(a): Revise "as are reasonable in the circumstances…" to "as are reasonable and necessary in the circumstances…".

[6] Biometric technologies are an emerging field, and many agencies will not have access to the necessary expertise to make sound judgements about the degree of risk involved and how these risks should be managed. In these cases, the precautionary principle should apply – i.e., the regulations should prevent agencies who lack the sophistication to conduct such an analysis from using biometric technology.

6. Who benefits?

6.1. The question of "who benefits?" from the deployment of biometric technology is not addressed sufficiently by the draft code. Agencies are required to "take into account whether the benefit of achieving the agency's lawful purpose by means of biometric processing outweighs the degree of privacy risk" (Rule 1(2)(d)). In turn, as outlined in section 3(4), the benefits of biometric processing are taken to outweigh privacy risks if one (or more) of the following conditions is met:

> (a) the public benefit outweighs the privacy risk; or
>
> (b) a clear benefit to the individuals concerned outweighs the privacy risk; or
>
> (c) the private benefit to the agency outweighs the privacy risk to a substantial degree.

6.2. We appreciate that the OPC's intention, as outlined in the consultation paper, is that "any public good or a clear advantage to the individual should be weighted higher than the benefits to the organisations". However, the current drafting would enable an employer to determine that the benefit to the organisation of, for example, using biometric trackables to increase worker productivity substantially outweighs the privacy risks that individual workers are exposed to by having to wear these trackables. But this does not mean that the workers themselves receive any benefits from the use of these biometric technologies. Thus, the employer, who does not incur any privacy risk, would get the returns from the technology, while the workers, who incur all the privacy risk, would get no returns. In other words, there will likely be cases in which the benefits to an employer are judged to substantially outweigh the risks to individual workers, but the distribution of these risks and benefits is highly unequal.

6.3. More fundamentally, the right to privacy is a fundamental right and it is therefore not necessarily able to be "weighed" against certain types of benefits, such as a business efficiency or an improved profit margin, as these belong to different categories of importance. As it currently stands, the proportionality test provisions encourage an accounting approach to be taken to assessing the risks and benefits of deploying biometric technology. But this accounting approach lumps fundamental rights in with other interests, such as commercial interests; these are not directly comparable, and it is therefore inappropriate to "weigh" them against one another.

6.4. To address this issue, we recommend that:

- An agency should have to assess not only the degree of privacy risk from the type of biometric processing, but also *how these risks are distributed* – i.e., who bears the risk.

- Agencies should have to meet specific requirements if biometric information is to be collected in the context of an employment relationship. Specifically, biometric information should not be collected from workers unless the privacy risks to those workers are outweighed by the benefits to those same workers.

7. Legitimate collection of information

7.1. We support the expectations outlined in Rule 3 and Rule 4. These set clear obligations on employers to proactively inform workers about the collection of their biometric data, its use and storage, and their rights under the Privacy Act.

7.2. However, there are several areas where these rules need to be strengthened if workers' privacy is to be effectively protected by the code of practice.

7.3. First, we are concerned by the provisional nature of Rule 3(1) – i.e., that agencies must only take steps that are "in the circumstances reasonable". To ensure that workers are protected from unscrupulous data collection/processing practices, we recommend that a further clause is added to this section which makes the conditions set out in Rule 3(1) *mandatory* if biometric information is being collected in the context of an employment relationship.

7.4. Second, we are concerned by the omission of a general (or specific) consent requirement from the draft code. Rule 1(1)(c) only requires that agencies adopt or implement "such privacy safeguards as are reasonable in the circumstances (if any)". In turn, section 3(3) references consent (although does not use the term itself) in the examples of privacy safeguards. In the employment context, this provides employers with significant latitude to collect and process biometric information in the workplace without first gaining consent from workers to do so. The employer can simply determine that it is not reasonably practicable to seek consent from their employees to gather and process their biometric information. The OPC's own analysis in the consultation papers would support such a determination.

7.5. The rationale given by the OPC for not making consent a general requirement is two-fold:

- First, due to the wide range of contexts in which biometric data may be collected, the OPC notes that it is difficult to develop a consent requirement that works in a broad range of contexts and in situations in which voluntary consent may be hard to achieve, such as in an employment relationship.

- Second, there is a risk that consent requirements would be "overlooked by consumers" who have "busy lives". To support this argument, the OPC cites an article from legal scholars Richards and Hartzog.[7]

7.6. To the first point, although it may be difficult to develop a single consent requirement that works in a broad range of contexts and situations, we see no reason why this should preclude specific consent requirements that are mandatory in certain contexts from being included in the code of practice. We recommend the employment relationship is one such context.

7.7. To the second point, we note that the scholarship cited by the OPC in support of this argument is explicitly focused on one context, that of digital consumer privacy. As Richards and Hartzog rightly point out, consent is often an inadequate privacy protection tool in the online context, in which consumers are inundated with requests for consent, are strongly incentivised not to consider the risks involved, and may often be unable to conceptualise the risks in the first place. Online contexts therefore do not meet Richards and Hartzog's three preconditions for valid consent:

> First, the choice to be made must be infrequent (so as not to overload the capacity of our minds to make rational choices). Second, the harms which we might incur by granting consent must be vivid (i.e., they must be easy to imagine). Third, the stakes of a decision to consent must be significant (i.e., there is ample incentive to take each decision seriously).[8]

7.8. However, these preconditions for consent can be more effectively realised in the employment context. To Richard and Hartzog's first criterion, it reasonable to expect that employer requests to collect/process biometric information in the workplace would be infrequent. Indeed, frequent requests from an employer to collect/process biometric information in the workplace would suggest excessive use of biometric technology. Richard and Hartzog's second and third criterions can be met by ensuring that any decision around the collection/processing of biometric information in the workplace is undertaken via good faith engagement with workers and that sufficient information is provided to workers regarding the serious nature of biometric data, how the data would be used, known and potential risks of its collection and processing, and workers' privacy rights, among other things (see our recommendations above regarding the proportionality test).

[7] N. Richards and W. Hartzog, "The Pathologies of Digital Consent", *Washington University Law Review* 96 (2019).
[8] Richards and Hartzog, "The Pathologies of Digital Consent", p. 1466.

7.9. The OPC is right to point out that the power imbalance between employer and worker can undermine a worker's ability to provide valid consent. But given the fundamental questions of human dignity and freedom that biometric information is tied up with, and the potentially severe consequences of its misuse, the decision not to include a consent requirement in the code of practice creates the risk that, in some workplaces, workers will be stripped of their sense of agency over their own biometric information. Thus, our view is that informed consent should be treated as a *necessary but not sufficient* privacy safeguard for workers.

7.10. To address these issues, we recommend that a further section is added in Rule 3 requiring that an employer must not collect biometric information from an worker unless the worker has:

- Provided specific and express consent for each purpose of collection.[9]
- Been provided with the opportunity to seek advice and comment on the lawfulness of the collection.
- Been sufficiently informed of the potential value of their biometric information, the known and potential risks associated with the collection and processing of their biometric information, and the actions that will be taken to safeguard their biometric information.
- Been provided with reasonable alternatives to the collection of their biometric information, without penalty or threat of penalty.

7.11. Finally, Rule 4(1) is intended to protect against unfair or excessive collection practices, and for the most part looks fit for purpose. However, Rule 4(1)(b)(ii) provides agencies with the ability to test the boundaries of what is considered "unreasonable". In practice, it is likely that some organisations will look to push beyond the boundaries of what is considered reasonable, which would in turn have to be addressed via complaints to the Privacy Commissioner. Internationally, for example, there has been a disturbing increase in the use of biometric technologies by employers to generate data on worker activity *outside* of the workplace, often under the guise of corporate wellness programmes.[10] This

[9] Additionally, the OPC should consider the value of using expiry dates for consent. Upon expiry, people would be prompted to reconsider whether they still consent to the collection/processing of their biometric information. In the employment context, this should help to reduce the risk of function and scope creep and would support awareness of biometric data collection/processing that is occurring in the workplace.

[10] I. Ajunwa, K. Crawford, and J. Schultz, "Limitless Worker Surveillance", *California Law Review* 105 (2017); C. Brassart Olsen, "To Track or Not to Track? Employees' Data Privacy in the Age of Corporate Wellness, Mobile Health, and GDPR", *International Data Privacy Law* 10 (2020).

encroaches upon workers' right to disconnect and be unavailable. There are many barriers to workers raising complaints if they feel their rights are being infringed upon. We therefore recommend the inclusion of a provision that explicitly confines biometric data collection to the workplace and work hours.

8. Enforcement

8.1. We agree with the OPC's suggestion that the code of practice apply to any organisation that starts using biometrics after the code becomes law. We recommend that, for organisations that are already collecting biometric information they should have a *maximum* of six months to comply after the code becomes law.

8.2. More generally, we note that regulations are only useful if they can be effectively enforced. In this case, the OPC needs to be adequately resourced to *proactively* identify the illegal, improper, and unsafe use of biometric technology and information and to take appropriate action.

9. Other comments

9.1. Rule 10(3)(b)(i) allows an agency to use biometric information that was obtained in connection with one purpose for another purpose, provided that the information "is to be used in a form in which the individual concerned is not identified". This raises issues of scope creep. For example, this provision would allow an employer who has collected their employees' biometric information for the purpose of improving workplace health and safety to then use this biometric information for tracking employee time on task, provided that no individuals can be recognised. This runs counter to the principal that individuals are the ultimate owners of data about themselves,[11] and should be explicitly consulted and aware of each use to which their data is put. We recommend Rule 10(3)(b)(i) is deleted.

9.2. The exclusion of heartbeat from the definition of behavioural biometrics is potentially problematic in the employment context. Internationally, some firms have used heartbeat tracking devices for their workforce as part of corporate wellness programs.[12] This is quite

[11] P. J. Singh, *Economic Rights in a Data-Based Society: Collective Data Ownership, Workers' Rights, and the Role of the Public Sector* (Public Services International and Friedrich Ebert Stiftung, 2020).
[12] EPRS, *Data Subjects, Digital Surveillance, AI, and the Future of Work* (European Parliament, 2020).

different to a consumer choosing to purchase and wear a smart watch. We recommend that heartbeat is included in the definition of behavioural biometrics if it is collected in the employment context.

9.3. We note there are some risks associated with the OPC's suggestion to exclude "readily apparent expressions" from the definition of biometric classification. It is reasonable to exclude some forms of readily apparent expressions – for example, the detection of voice volume to auto-adjust audio levels. However, there is the risk that agencies will use this as a loophole to avoid having to comply with the code in areas where the line between readily apparent expression and inner psychological state is blurry. For example, facial expression tracking software could be used in retail contexts, to monitor if employees are comporting their face in a friendly or approachable manner. This would pressure employees into comporting their face in a particular manner, even if this was radically at odds with the inner psychological state they were currently experiencing. This compounds job stress and can be alienating for workers.

9.4. Finally, we recommend that the OPC commissions a study into the prevalence and types of biometric processing covered by the code that are occurring in New Zealand. We currently do not have a strong evidence base on the extent to which biometric technologies are being used in New Zealand, and this limits our ability to understand the types of privacy impacts it may be having.

10. Conclusion

10.1. The CTU thanks the Office of the Privacy Commissioner for the opportunity to submit on this important work.

10.2. The CTU is strongly supportive of the OPC issuing a code of practice on biometric processing. We have recommended a set of changes to the draft code that would, in our view, help to better protect workers from the privacy risks associated with biometric technologies.

10.3. Please see the Appendix, overleaf, for our suggested revisions to the draft code, where we have integrated the recommendations made above.

11. Appendix: Recommended revisions to the draft code

Section 3(3)

(3) In this code, **privacy safeguards** means actions or processes that are relevant and ~~reasonably practicable~~ necessary in the circumstances to reduce privacy risk, including any of the following measures—

Rule 1: Purpose of collection of biometric information

(1) Biometric information must not be collected by an agency unless—
- (a) the information is collected for a reasonable, legitimate, and **lawful purpose** connected with a function or an activity of the agency;
- (b) the collection of the information is **necessary** for that purpose;
- (c) the agency has adopted or implemented such **privacy safeguards** as are reasonable and necessary in the circumstances (if any); and
- (d) the agency ~~believes~~ has established, on reasonable grounds, that the biometric processing is not **disproportionate** in the particular circumstances.

(2) For purposes of subrule (1)(d), the agency must ~~take into account the following circumstances~~ produce a proportionality assessment that shall contain—
- (a) a description of the proposed method of biometric processing;
- (b) the date from which the proposed method of biometric processing would be used;
- (c) the logic which underpins the biometric processing system;
- (d) whether or not biometric processing is **effective** in achieving the agency's lawful purpose;
- (e) the degree of **privacy risk** from the type of biometric processing, and who carries these risks;
- (f) whether or not the agency's lawful purpose can reasonably be achieved by an **alternative** means to biometric processing, or by an alternative type of biometric processing, that has less privacy risk;
- (g) whether the **benefit** of achieving the agency's lawful purpose by means of biometric processing **outweighs** the degree of privacy risk;
- (h) the cultural impacts and effects of biometric processing on Māori; and
- (i) the cultural impacts and effects on any other New Zealand demographic group.

(3) For purposes of subrules (1)(c) and (1)(d), the agency must produce a risk assessment that shall contain—
- (a) a description of the proposed method of biometric processing;
- (b) the date from which the proposed method of biometric processing would be used;
- (c) the logic which underpins the biometric processing system;
- (d) the different privacy risks (if any) associated with the type of biometric processing;

(e) who is exposed to these privacy risks;
(f) the likelihood of these risks occurring;
(g) the consequences of these risks occurring;
(h) the privacy safeguards that are necessary to implement to prevent these risks occurring;
(i) how the agency will implement and maintain these privacy safeguards; and
(j) the agency's capacity to implement and maintain these privacy safeguards.

(4) If biometric processing is to be used in the context of an employment relationship—
(a) the proportionality assessment provided for in subrule (2) and the risk assessment provided for in subrule (3) must be developed in consultation with workers and employees who may be affected;
(b) the proportionality assessment provided for in subrule (2) and the risk assessment provided for in subrule (3) must be developed in consultation with persons who are appropriate representatives of the workers and employees who may be affected; and
(c) biometric information must not be collected from workers and employees unless the privacy risks to those workers and employees are shown to be outweighed by benefits to those same workers and employees.

(5) For purposes of subrule (4), consultation must take into account all legitimate concerns and interests of workers and employees who may be affected by biometric processing, including—
(a) understanding and minimising any privacy risks associated with biometric processing; and
(b) the impact or potential impact of biometric processing upon workers and employees in relation to their wellbeing.

(6) For the purposes of subrule (4)(a), workers and employees who may be affected by biometric processing must be provided with a copy of the proportionality assessment and risk assessment.

(7) For purposes of subrule (4)(b) the legitimate representatives of workers and employees who may be affected by biometric processing must be provided with a copy of the proportionality assessment and risk assessment.

(8) If the lawful purpose for which biometric information is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information.

Rule 3: Collection of information from individual

(1) If an agency collects a biometric sample for biometric processing from the individual concerned, the agency must take steps that are, in the circumstances reasonable to ensure that the individual concerned is aware of—
  (a) the fact that the biometric information is being collected; and
  (b) each specific purpose or purposes for which the biometric information is being collected, specified with due particularity; and
  (c) the intended recipients of the biometric information; and
  (d) the name and address of—
    (i) the agency that is collecting the biometric information; and
    (ii) the agency that will hold the biometric information; and
  (e) if the collection of the biometric information is authorised or required by or under law—
    (i) the particular law by or under which the collection of the biometric information is authorised or required; and
    (ii) whether the supply of the biometric information by the individual is voluntary or mandatory; and
  (f) the consequences (if any) for that individual if all or any part of the requested biometric information is not provided; and
  (g) the rights of access to, and correction of, information provided by rules 6 and 7; and
  (h) whether there is any alternative option to biometric processing that is available to the individual in any particular circumstances; and
  (i) a summary of the agency's retention policy for biometric information;
  (j) the process, if any, provided by the agency for an individual to:
    (i) raise a concern about biometric processing including the handling of their biometric information; and
    (ii) make a complaint about the handling of their biometric information; and
  (k) the right to complain to the Privacy Commissioner about any action that this code applies to; and
  (l) the particular law by or under which the use or disclosure of the biometric information is authorised or required, if the use or disclosure is authorised or required by or under New Zealand law, including an authorised information sharing agreement, or the laws of another country; and
  (m) a list of the agency's policies, protocols and procedures, if any, that apply to the agency's use and disclosure of biometric information.

(2) The steps referred to in subrule (1) must include—
  (a) an **accessible notice** that includes the matters specified in subrule (1); and
  (b) a **conspicuous notice** that includes the matters specified in subrule (1)(a), (b) and (h).

(3) The steps referred to in subrules (1) and (2)(a) must be taken before the biometric information is collected or, if that is not practicable, as soon as practicable after the biometric information is collected.

(4) The steps referred to in subrule (2)(b) must be taken before the biometric information is collected.

(5) If an employer intends to collect biometric information from their workers and employees—
- (a) the steps referred to in subrule (1) must be taken;
- (b) workers and employees must provide specific and express consent for each purpose of collection;
- (c) collection may only take place within the agreed place of work and within agreed work hours.

(6) For purposes of subrule (5)(b), consent is only considered valid if workers and employees are—
- (a) provided with all information referred to in subrule (1);
- (b) provided with the proportionality assessment and risk assessment required under Rule 1.
- (c) provided with the opportunity to seek advice and comment on the lawfulness of the collection;
- (d) informed of the value of their biometric information;
- (e) informed of the risks associated with the processing of their biometric information;
- (f) provided with reasonable alternatives to the collection of their biometric information, without penalty or threat of penalty.

(7) It is not necessary for an agency to comply with subrules (1) or (2) if the agency believes on reasonable grounds—
- (a) that non-compliance is necessary—
  - (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
  - (ii) for the enforcement of a law that imposes a pecuniary penalty; or
  - (iii) for the protection of public revenue; or
  - (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
- (b) that compliance would prejudice the purposes of the collection.

(8) Without limiting subrule (5), it is not necessary for the agency to comply with sub-rule (2)(b) (in full or in part) if the agency believes on reasonable grounds—
- (a) that compliance is not reasonably practicable in the circumstances of the particular case; or

(b) that the biometric information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

(9) An agency is not required to take the steps referred to in subrules (1) or (2)(a) in relation to the collection of biometric information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind.

Rule 5: Storage and security of biometric information

An agency that holds biometric information must ensure,—

(a) that the information is protected, by such security safeguards as are reasonable and necessary in the circumstances to take, against—
  (i) loss; and
  (ii) access, use, modification, or disclosure that is not authorised by the agency; and
  (iii) other misuse; and

(b) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Rule 10: Limits on use of biometric information

(1) An agency that holds a biometric sample may not use the information in biometric processing or for a different type of biometric processing for any purpose unless—
  (a) the agency has adopted or implemented such privacy safeguards as are reasonable in the circumstances (if any); and
  (b) the agency believes, on reasonable grounds, that the type of biometric processing is not disproportionate in the particular circumstances.

(2) For purposes of subrules (1)(b), the agency must take into account the circumstances in rule 1(3).

(3) Without limiting sub-rule (1), an agency that holds biometric information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds,—
  (a) that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or
  (b) that the information—
    ~~(i) is to be used in a form in which the individual concerned is not identified;~~
    ~~or~~

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(c) that the use of the information for that other purpose is authorised by the individual concerned; or

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or

(e) that the use of the information for that other purpose is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law that imposes a pecuniary penalty; or

(iii) for the protection of public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual.

(4) In addition to the uses authorised by subrule (3), an intelligence and security agency that holds biometric information that was obtained in connection with one purpose may use the information for any other purpose (a **secondary purpose**) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.