**BIOMETRIC PROCESSING PRIVACY CODE**

**EXPOSURE DRAFT ONLY**

**FOR COMMENT**

**Contents**

Part 1: Preliminary

1. Title
2. Commencement
3. Interpretation
4. Application of code

Part 2: Biometric processing information privacy rules

1. Biometric processing information privacy

Rule 1: Purpose of collection of biometric information

Rule 2: Source of biometric information

Rule 3: Collection of information from individual

Rule 4: Manner of collection of biometric information

Rule 5: Storage and security of biometric information

Rule 6: Access to biometric information

Rule 7: Correction of biometric information

Rule 8: Accuracy etc of biometric information to be checked before use or disclosure

Rule 9: Retention of biometric information

Rule 10: Limits on use of biometric information

Rule 11: Limits on disclosure of biometric information

Rule 12: Disclosure of biometric information outside New Zealand

Rule 13: Unique identifiers

Part 1: Preliminary

1. **Title**

This code of practice is the Biometric Processing Privacy Code [*year*].

1. **Commencement**

This code comes into force—[[1]](#footnote-1)

1. on [*day/month/year*] for any type of biometric processing that has not commenced before that date; or
2. on [*6 months later*] for any type of biometric processing that commenced before [*date in (a)*].
3. **Interpretation**
4. In this code,—

**access limit[[2]](#footnote-2)** means a limit on an individual’s access to goods or services, to a physical or online location, or to any particular content

**accessible notice**[[3]](#footnote-3)means a notice in plain language, including an online notice, that is—

1. readily accessible to the individuals concerned; and
2. presented independently of an agency’s privacy statement

**accessibility[[4]](#footnote-4)** means actions, measures, modifications or adjustments that help enable individuals with a disability to overcome or reduce barriers to participation on an equal basis with others

**adverse action[[5]](#footnote-5)** means any action, informed by a biometric result, with respect to any specified individual—

1. to monitor or profile the individual, including surveillance of the individual; or
2. that may adversely affect the individual’s rights, benefits, privileges, obligations, or interests including the imposition of a penalty or a fine; or
3. that may cause loss, detriment, damage or injury to the individual; or
4. that may result in humiliation, loss of dignity or injury to feelings of the individual

**behavioural biometric[[6]](#footnote-6)** means a measurement or record of the way that an individual characteristically performs or responds to a task, action or decision with any part of their body including—

1. the individual’s gestures, gait, voice, eye movements, signature or handwriting style; and
2. the individual’s pattern of using any digital device;

**benefit** has the meaning in subclause (4)

**biological material**[[7]](#footnote-7) means—

1. the whole or part of any organ, bone, tissue, or cell; or
2. blood or body fluids

**biometric category[[8]](#footnote-8)** means a group or class of individuals that share a common attribute, including a category based on the individual’s age, race, ethnicity, or gender

**biometric classification[[9]](#footnote-9)** means the process of analysing a behavioural biometric or a physiological biometric to infer or detect, or to attempt to infer or detect—

1. health information about an individual; or
2. information about an individual’s inner state or physical state; or
3. information to categorise the individual according to one or more biometric categories;

but does not include any analytical process that is integrated in a commercial service and is solely dependent on that service, cannot be used separately from it, and where the effect of the integration does not circumvent the rules in this code[[10]](#footnote-10)

**biometric identification[[11]](#footnote-11)** means the process of seeking to identify an individual by means of a biometric search

**biometric information[[12]](#footnote-12)** means any of the following types of personal information, in connection with any type of biometric processing—

1. a behavioural biometric;
2. a physiological biometric;
3. a biometric sample;
4. a biometric template; and
5. a biometric result;

but does not include any information obtained or inferred from—

1. the individual’s biological material;
2. the individual’s genetic material;
3. the individual’s brain activity; or
4. the individual’s nervous system

**biometric processing[[13]](#footnote-13)** means the comparison or analysis of biometric information by a biometric system that produces a biometric result, and includes the following types of biometric processing—

1. biometric identification;
2. biometric verification; and
3. biometric classification

**biometric query[[14]](#footnote-14)** means a biometric sample or a biometric template that is used as an input in a biometric search

**biometric reference[[15]](#footnote-15)** means any stored biometric sample or a biometric template that is used as the object of comparison in a biometric search

**biometric result[[16]](#footnote-16)** includes a comparison decision, biometric category or other result of biometric processing including an alert, prediction, analysis, assessment, determination, recommendation, identification, calculation or inference about an individual, whether or not the result is accurate or inaccurate, false, misleading, or is a false positive or a false negative

**biometric sample[[17]](#footnote-17)** means an analogue or digital record of an individual’s behavioural biometric or physiological biometric

**biometric search** means the action of comparing a biometric query with one or more biometric references to make a comparison decision

**biometric system** means a machine-based system, including any computer software, application or algorithm, that is used for biometric processing or a type of biometric processing, regardless of whether the system involves human input, assistance or oversight, and does not include a system that relies solely or primarily on human analysis[[18]](#footnote-18)

**biometric template[[19]](#footnote-19)** meansa numerical or algorithmic representation of information extracted from a biometric sample

**biometric verification[[20]](#footnote-20)** means the process of seeking to verify the identity of an individual by means of a biometric search

**biometric watchlist[[21]](#footnote-21)** means a database of biometric references used in biometric identification for the purpose of deciding whether to take an adverse action

**comparison decision[[22]](#footnote-22)** means a decision resulting from a biometric search assessing the likelihood that a biometric query and a biometric reference relate to the same individual, and includes any positive match, probable match, and non-match

**conspicuous notice[[23]](#footnote-23)** means a written or verbal notice in plain language—

1. that is displayed or presented in a location where it can be readily noticed by individuals before their biometric information is collected or at the point of collection; and
2. that includes a location or address for, or means of an individual obtaining, an accessible notice; and
3. that is presented independently of an accessible notice or an agency’s privacy policy;

and includes a physical notice or an online notice

**disability[[24]](#footnote-24)** has the meaning in section 21(1)(h) of the Human Rights Act 1993

**health agency[[25]](#footnote-25)** has the meaning in the Health Information Privacy Code 2020

**heath information[[26]](#footnote-26)** has the meaning in the Health Information Privacy Code 2020

**inner state[[27]](#footnote-27)** means an individual’s personality, mood, emotion, intention, or mental state and does not include—

1. an individual’s physical state; or
2. detection of a readily apparent expression

**physical state[[28]](#footnote-28)** means an individual’s state of fatigue, alertness, or attention level

**physiological biometric[[29]](#footnote-29)** means a measurement or record of the physical appearance of any part of an individual’s body including their face, fingerprints, palmprints, iris, retina, or vein patterns

**plain language[[30]](#footnote-30)** has the meaning in section 5 of the Plain Language Act2022[[31]](#footnote-31)

**privacy breach[[32]](#footnote-32)** has the meaning in section 112 of the Act

**privacy risk** has the meaning in sub-clause (2)

**privacy safeguards** has the meaning in sub-clause (3).

**protected rights**[[33]](#footnote-33)means the rights protected under the New Zealand Bill of Rights Act 1990

**readily apparent expression[[34]](#footnote-34)** means an individual's expression, gesture, movement or the level or pitch of their voice that can be observed or recorded visually or aurally without biometric processing

**restricted biometric category[[35]](#footnote-35)** means a biometric category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993, other than the age of the individual concerned

**rule** means a biometric processing privacy rule set out in Part 2 of this code

**the Act** means the Privacy Act 2020

**web scraping[[36]](#footnote-36)** means using automated tools to extract biometric information from publicly available online sources including websites and social media platforms

1. In this code, **privacy risk**[[37]](#footnote-37) is any reasonable likelihood that the privacy of individuals may be infringed by—
2. biometric processing; or
3. any action[[38]](#footnote-38) relating to biometric processing;[[39]](#footnote-39) or
4. an alternative to biometric processing;[[40]](#footnote-40)

and includes the following risks—

1. the collection of biometric information that is not necessary for a particular purpose; (*over collection*)
2. the retention of biometric information for longer than is necessary for a particular purpose; (*over retention*)
3. biometric information is not accurate, up to date, complete, relevant, or is misleading; (*inaccuracy*)
4. the misidentification or misclassification of an individual, including where any such risk is variable based on attributes such as the individual’s race, ethnicity, gender, sex, age or disability (whether separately or in combination); (*bias*)
5. biometric information is vulnerable to a privacy breach; (*security vulnerability*)
6. the individual is not aware of the collection of biometric information or does not understand the purposes of biometric processing; (*lack of transparency*)
7. biometric processing for the purposes of surveillance, monitoring or profiling may result in any adverse action or deter the individual from exercising any protected rights; (*chilling effect)*
8. the expansion of the purposes for which biometric information may be used or disclosed following the collection of the information. (*scope creep*)
9. In this code, **privacy safeguards**[[41]](#footnote-41) means actions or processes that are relevant and reasonably practicable in the circumstances to reduce privacy risk, including any of the following measures—

1. individuals are able to authorise the biometric processing, based on an informed decision, or are able to opt out of biometric processing;
2. where a biometric system operates a biometric watchlist, the individual concerned is informed:
   1. when the individual is enrolled in the biometric system;
   2. how the individual may challenge their enrolment;
   3. if an adverse action is taken or is to be taken; and
   4. how the individual may challenge a decision to take an adverse action;
3. the biometric system has been subjected to testing and/or assurance processes prior to biometric processing;
4. biometric information is protected by reasonable security safeguards against the risk of a privacy breach, including where it is necessary for biometric information to be given to a person in connection with the provision of a service to an agency;
5. the biometric system has trained human oversight or monitoring to ensure the monitoring, recording and correction of flawed biometric results, including false positives or false negatives, and resulting actions;
6. biometric processing is subject to regular review and audit to monitor and identify privacy risk and to ensure that the intended safeguards remain effective;
7. training of relevant staff is complete and up to date before biometric information is collected or used; and
8. biometric processing and the operation of any biometric watchlist is carried out in accordance with protocols, policies and procedures that are readily accessible to relevant staff, regularly reviewed and kept up to date.
9. For purposes of this code, the **benefit**[[42]](#footnote-42) of an agency achieving its lawful purpose outweighs the privacy risk of biometric processing if, in the circumstances—
10. the public benefit outweighs the privacy risk; or
11. a clear benefit to the individuals concerned outweighs the privacy risk; or
12. the private benefit to the agency outweighs the privacy risk to a substantial degree.
13. A term or expression defined in section 7 of the Act and used, but not defined in this code has the same meaning as the Act.
14. **Application of code**
15. This code applies to:
16. the activity of **biometric processing**; and
17. **biometric information** as a class of information for purposes of that activity.[[43]](#footnote-43)
18. This code does not apply to the activity of biometric processing by a **health agency** or to biometric information as a class of information for purposes of that activity if the biometric information is **health information**.[[44]](#footnote-44)
19. Rules 2, 3, 4(1)(b), 4(2) and 4(3) do not apply to an intelligence and security agency.[[45]](#footnote-45)

Part 2: Biometrics Processing Privacy Rules

1. **Biometric processing privacy rules**

In accordance with the Act, the following rules modify the application of the information privacy principles, prescribe how some of the principles are to be applied or complied with and apply some principles without modification:

**Rule 1**  
**Purpose of collection of biometric information[[46]](#footnote-46)**

1. Biometric information must not be collected by an agency unless—
2. the information is collected for a **lawful purpose** connected with a function or an activity of the agency;
3. the collection of the information is **necessary** for that purpose;
4. the agency has adopted or implemented such **privacy safeguards** as are reasonable in the circumstances (if any); and
5. the agency believes, on reasonable grounds, that the biometric processing is not **disproportionate** in the particular circumstances.
6. For purposes of subrule (1)(d), the agency must take into account the following circumstances—
7. whether or not biometric processing is **effective** in achieving the agency’s lawful purpose;
8. the degree of **privacy risk** from the type of biometric processing;
9. 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;
10. whether the **benefit** of achieving the agency’s lawful purpose by means of biometric processing **outweighs** the degree of privacy risk;
11. the cultural impacts and effects of biometric processing on Māori; and
12. the cultural impacts and effects on any other New Zealand demographic group.
13. 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.[[47]](#footnote-47)

**Rule 2  
Source of biometric information[[48]](#footnote-48)**

1. If an agency collects a biometric sample for biometric processing, the information must be collected from the individual concerned.
2. It is not necessary for an agency to comply with subrule (1) if the agency believes, on reasonable grounds,—
3. that compliance would prejudice the interests of the individual concerned; or
4. that compliance would prejudice the purposes of the collection; or
5. that the individual concerned authorises collection of the information from someone else; or
6. that the information is publicly available information; or
7. that non-compliance is necessary—
8. 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
9. for the enforcement of a law that imposes a pecuniary penalty; or
10. for the protection of public revenue; or
11. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
12. to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual; or
13. that compliance is not reasonably practicable in the circumstances of the particular case; or
14. that the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) 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.

1. Rule 2(2)(d) does not permit the collection of a biometric sample by means of web scraping.

**Rule 3  
Collection of information from individual[[49]](#footnote-49)**

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—
2. the fact that the biometric information is being collected; and
3. each specific purpose or purposes for which the biometric information is being collected, specified with due particularity; and
4. the intended recipients of the biometric information; and
5. 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

1. 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

1. the consequences (if any) for that individual if all or any part of the requested biometric information is not provided; and
2. the rights of access to, and correction of, information provided by rules 6 and 7; and
3. whether there is any alternative option to biometric processing that is available to the individual in any particular circumstances; and
4. a summary of the agency’s retention policy for biometric information;
5. 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

1. the right to complain to the Privacy Commissioner about any action that this code applies to; and
2. 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
3. a list of the agency’s policies, protocols and procedures, if any, that apply to the agency’s use and disclosure of biometric information.
4. The steps referred to in subrule (1) must include—
5. an **accessible notice** that includes the matters specified in subrule (1); and
6. a **conspicuous notice** that includes the matters specified in subrule (1)(a), (b) and (h).
7. 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.
8. The steps referred to in subrule (2)(b) must be taken before the biometric information is collected.
9. It is not necessary for an agency to comply with subrules (1) or (2) if the agency believes on reasonable grounds—
10. 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

1. that compliance would prejudice the purposes of the collection.
2. 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—
3. that compliance is not reasonably practicable in the circumstances of the particular case; or
4. 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.
5. 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 4  
Manner of collection of biometric information[[50]](#footnote-50)**

1. An agency may collect biometric information only—
2. by a lawful means; and
3. by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or other young persons),—

(i) is fair; and

(ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

1. Without limiting subrule (1), an agency may not use biometric classification to collect any of the following types of personal information, —
2. health information; or
3. information about an individual’s inner state or physical state; or
4. information about an individual to categorise the individual according to—
   1. a **restricted biometric category;** or
   2. the age of the individual concerned.
5. It is not necessary for an agency to comply with subrule (2) if, in the circumstances of the case the agency believes on reasonable grounds—
6. that the collection of information about the individual’s physical state is necessary to meet health and safety standards; or
7. that the collection of information to categorise the individual concerned according to their age is necessary in order to comply with a lawful obligation or duty to apply an access limit or to meet a duty of care owed to the individual; or
8. that the collection of information is necessary to assist an individual with **accessibility**;
9. that the collection of information 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; or

1. the collection of information is for statistical or research purposes if—

(i) the collection is conducted with ethical oversight, ethics approval and with the written authorisation of the individual concerned or the individual’s authorised representative; and

(ii) the agency believes, on reasonable grounds, that the statistics or research will not be published in a form that could reasonably be expected to identify the individual concerned.

**Rule 5  
Storage and security of biometric information**

An agency that holds biometric information must ensure,—

1. that the information is protected, by such security safeguards as are reasonable 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

1. 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 6  
Access to biometric information[[51]](#footnote-51)**

1. An individual is entitled to receive from an agency upon request—
2. confirmation of whether the agency holds any biometric information about them; and
3. confirmation of the type of biometric information the agency holds about them; and
4. access to their biometric information.
5. If an individual concerned is given access to biometric information, the individual must be advised that, under IPP 7, the individual may request the correction of that information.
6. This rule is subject to the provisions of [Part 4](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23421.html#LMS23421) of the Act.

**Rule 7  
Correction of biometric information**

1. An individual whose biometric information is held by an agency is entitled to request the agency to correct the information.
2. An agency that holds biometric information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.
3. When requesting the correction of biometric information, or at any later time, an individual is entitled to—
4. provide the agency with a statement of the correction sought to the information (a **statement of correction**); and
5. request the agency to attach the statement of correction to the information if the agency does not make the correction sought.
6. If an agency that holds biometric information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.
7. If an agency corrects biometric information or attaches a statement of correction to biometric information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.
8. Subrules (1) to (4) are subject to the provisions of [Part 4](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23421.html#LMS23421) of the Act.

**Rule 8  
Accuracy, etc, of biometric information to be checked before use or disclosure**

An agency that holds biometric information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

**Rule 9  
Retention of biometric information**

An agency that holds biometric information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

**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—[[52]](#footnote-52)
2. the agency has adopted or implemented such privacy safeguards as are reasonable in the circumstances (if any); and
3. the agency believes, on reasonable grounds, that the type of biometric processing is not disproportionate in the particular circumstances.
4. For purposes of subrules (1)(b), the agency must take into account the circumstances in rule 1(3).
5. 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,—
6. 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
7. 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

1. that the use of the information for that other purpose is authorised by the individual concerned; or
2. 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
3. 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

1. 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.

1. 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.

**Rule 11  
Limits on disclosure of biometric information[[53]](#footnote-53)**

1. An agency that holds biometric information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds,—
2. that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
3. that the disclosure is to the individual concerned; or
4. that the disclosure is authorised by the individual concerned; or
5. that the source of the information is a publicly available publication and that, in the circumstances of the case,

(i) the information has not been obtained by means of web scraping, in the case of a biometric sample; or

(ii) it would not be unfair or unreasonable to disclose the information; or

1. that the disclosure of the information 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

1. that the disclosure of the information 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; or

1. that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or
2. 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

1. that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.
2. This rule is subject to rule 12.

**Rule 12  
Disclosure of biometric information outside New Zealand**

1. An agency (**A**) may disclose biometric information to a foreign person or entity (**B**) in reliance on rule 11(1)(a), (c), (e), (f), (h), or (i) only if—
2. The individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act, as modified by this code; or
3. B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act, as modified by this code; or
4. A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act, as modified by this code; or
5. A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or
6. A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or
7. A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act, as modified by this code (for example, pursuant to an agreement entered into between A and B).
8. However, subrule (1) does not apply if the biometric information is to be disclosed to B in reliance on rule 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subrule (1).
9. In this rule,—

**prescribed binding scheme** means a binding scheme specified in regulations made under [section 213](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS151131.html#LMS151131) of the Act.

**prescribed country** means a country specified in regulations made under [section 214 of the Act](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS138198.html#LMS138198) that are made without any qualification or limitation relating to a class of person that includes B, or to a type of information that includes biometric information.

**Rule 13  
Unique Identifiers**

1. An agency (**A**) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.
2. A may not assign to an individual a unique identifier and that, to A’s knowledge, is the same unique identifier as has been assigned to that individual by another agency (**B**), unless—
3. A and B are associated persons within the meaning of [subpart YB](https://www.legislation.govt.nz/act/public/2007/0097/latest/DLM1522997.html#DLM1522997) of the Income Tax Act 2007; or
4. the unique identifier is to be used by A for statistical or research purposes and no other purpose.
5. To avoid doubt, A does not assign a unique identifier to an individual under subrule (1) by simply recording a unique identifier assigned to the individual by B for the sole purpose of communicating with B about the individual.
6. A must take any steps that are, in the circumstances, reasonable to ensure that—
7. a unique identifier is assigned only to any individual whose identity is clearly established; and
8. the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).
9. An agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.

1. Clause 2(a) proposes an immediate commencement for new processing use cases that are initiated on or after the code is issued. Clause 2(b) proposes a deferred 6-month commencement period for existing processing use cases to allow time to comply with code requirements. [↑](#footnote-ref-1)
2. **Access limits** (based on age) are an exception (rule 4(3)(b)) to the proposed limit on using **biometric classification** to collect information about an individual’s age in rule 4(2)(c). [↑](#footnote-ref-2)
3. A type of notice to be given under rule 3(2) when a **biometric sample** is collected from an individual. [↑](#footnote-ref-3)
4. **Accessibility** is an exception (rule 4(3)(c)) to the proposed limit on using **biometric classification** to collect information about **restricted biometric categories** in rule 4(2)(c). [↑](#footnote-ref-4)
5. This term is used in the definition of **biometric watchlist**, and in the definitions of **privacy risk** in clause 3(2)(vii) and **privacy safeguard** in clause 3(3)(b). [↑](#footnote-ref-5)
6. A type of **biometric information** that is an input into **biometric processing**. See also **physiological biometric** as the other type of biometric input. [↑](#footnote-ref-6)
7. This type of information is excluded from the definition of **biometric information** and is therefore outside the scope of the proposed code. [↑](#footnote-ref-7)
8. This term is used in the definition of **biometric classification**, one of the three types of **biometric processing**. [↑](#footnote-ref-8)
9. One of three types of **biometric processing**. Limits on using **biometric classification** are proposed in rule 4(2), with exceptions in rule 4(3). [↑](#footnote-ref-9)
10. The intent of the exclusion is to exclude mundane categorisation such as filters, or face detection. Compare EU AI Act for similar exclusion. [↑](#footnote-ref-10)
11. One of three types of **biometric processing**. [↑](#footnote-ref-11)
12. A key definition in denoting the proposed scope of the code and rules. [↑](#footnote-ref-12)
13. A key definition in denoting the proposed scope of the code and rules. [↑](#footnote-ref-13)
14. This term is used to refer to the biometric inputs into a **biometric search** for **biometric processing** to compare against **biometric references** held in the **biometric system**. [↑](#footnote-ref-14)
15. This term is used to refer to the biometric records that are stored for comparison against **biometric samples** and **biometric templates** through a **biometric search**. [↑](#footnote-ref-15)
16. The outcome of **biometric processing** and a type of **biometric information**. [↑](#footnote-ref-16)
17. A type of **biometric information**, covering both **behavioural** **biometrics** and **physiological biometrics**, that are inputs into **biometric processing**. [↑](#footnote-ref-17)
18. This excludes manual biometric processing from the scope of the proposed code. [↑](#footnote-ref-18)
19. A category of **biometric information**. [↑](#footnote-ref-19)
20. One of three types of **biometric processing**. [↑](#footnote-ref-20)
21. This term is used in the definition of **privacy safeguards** in clause 3(3)(b) and (h). [↑](#footnote-ref-21)
22. A step in **biometric processing** that is **biometric identification** or **biometric verification**, and a type of **biometric result** following a **biometric search**. [↑](#footnote-ref-22)
23. A type of notice to be given under rule 3(2) when a **biometric sample** is collected from an individual. [↑](#footnote-ref-23)
24. This term is used in the definition of **accessibility** and in the definition of **privacy risk** in clause 3(2)(iv). [↑](#footnote-ref-24)
25. Clause 4 proposes that the application of the code would not extend to **health agencies** for activities covered by the Health Information Privacy Code 2020. [↑](#footnote-ref-25)
26. Rule 4(2) proposes limits on using **biometric classification** to collect or infer **health information**. This term is also used in the definition of **biometric classification**. [↑](#footnote-ref-26)
27. Rule 4(2) proposes limits on using **biometric classification** to collect or infer information about a person’s mood or emotion (**inner state**). This term is also used in the definition of **biometric classification**. [↑](#footnote-ref-27)
28. Collecting information about an individual’s **physical state** for purposes of health and safety is an exception (rule 4(3)(a)) to the proposed limit on using biometric classification in rule 4(2)(b). [↑](#footnote-ref-28)
29. A type of **biometric information** that is an input into **biometric processing**. See also **behavioural biometric** as the other type of biometric input. [↑](#footnote-ref-29)
30. Term used in the definitions of **accessible notice** and **conspicuous notice** for rule 3(2). [↑](#footnote-ref-30)
31. **Plain language** is defined in the Plain Language Act as meaning language that is—

    ##### *(a) appropriate to the intended audience; and*

    ##### *(b) clear, concise, and well organised*.

    [↑](#footnote-ref-31)
32. This term is used in the definition of **privacy risk** in clause 3(2)(v). [↑](#footnote-ref-32)
33. This term is used in the definition of **privacy risk** in clause 3(2)(vii). [↑](#footnote-ref-33)
34. An exception in the definition of **inner state** and therefore an exception to the proposed limit on using **biometric classification** to infer an individual’s mood or emotion – rule 4(2). [↑](#footnote-ref-34)
35. Rule 4(2) proposes limits on using **biometric classification** to collect or inferinformation to categorise an individual according to a **restricted biometric category** or on the basis of age. [↑](#footnote-ref-35)
36. This term is used in rule 2(3) and limits the exception in rule 2(2)(d) for collecting a **biometric sample** that is publicly available information. See also rule 11(d)(i) and the limit on disclosing biometric information if the source is a **biometric sample**. [↑](#footnote-ref-36)
37. **Privacy risk** is one of the inputs into the proposed proportionality assessment required for **biometric processing** in rule 1(1)(d) and rule 10(1)(b). [↑](#footnote-ref-37)
38. This term is defined in the Privacy Act 2020 and includes any policy or practice, and any failure to act. [↑](#footnote-ref-38)
39. For example, the collection of **biometric information** in advance of processing, developing protocols and processes, or establishing a **biometric watchlist**. [↑](#footnote-ref-39)
40. This limb is included to allow for the **privacy risk** of a non-automated (manual) processing option to be assessed when comparing alternatives to **biometric processing** for the proportionality assessment under rules 1(1)(d) and 10(1)(b) as required by the proposed factor in rule 1(2)(c). [↑](#footnote-ref-40)
41. **Privacy safeguards** are to be considered under rule 1(1)(c) and rule 10(1)(a). [↑](#footnote-ref-41)
42. **Benefit** is one of the inputs into the proportionality assessment for **biometric processing** in rule 1(1)(d) and rule 10(1)(b). The proposed factor in rule 1(3)(d) would require a comparison of the degree of **privacy risk** with the degree of **benefit** from **biometric processing**. [↑](#footnote-ref-42)
43. The scope of the proposed code excludes manual biometric processing, as the definition of **biometric system** (used in the definition of **biometric processing**) relates to automated processing. [↑](#footnote-ref-43)
44. Clause 4(2) proposes that the application of the code would not extend to **health agencies** for activities covered by the Health Information Privacy Code 2020. [↑](#footnote-ref-44)
45. As per section 28 of the Privacy Act 2020. [↑](#footnote-ref-45)
46. Rule 1 proposes that the threshold for **biometric processing** would include an assessment of **privacy safeguards** in rule 1(1)(c) and a proportionality assessment in rule 1(1)(d), including the factors in rule 1(2). [↑](#footnote-ref-46)
47. This mirrors IPP1(2) in the Privacy Act, requiring consideration of whether the collection of identifiers is necessary. While this will not be applicable in the case of some types of **biometric processing** such as **biometric identification**, it may be relevant in other cases such as **biometric classification**. [↑](#footnote-ref-47)
48. Rule 2 applies to the collection of **biometric samples** from individuals and proposes a limit in rule 2(3) on **web scraping** to the exception available for collecting **biometric samples** that are publicly available information (for example photographs). [↑](#footnote-ref-48)
49. Rule 3 proposes additional matters to be notified to the individual on the collection of **biometric sample** in rule 3(1)(h)-(m), and proposes certain notification steps to be taken in rule 3(2). The exceptions to notification are tailored in rule 3(5) - (7). [↑](#footnote-ref-49)
50. Rule 4(2) proposes limits on the use of **biometric classification** to infer **health information** or to infer mood or emotion (**inner state**) or to classify individuals on the basis of their age or a **restricted biometric category**, in each case, subject to relevant exceptions in rule 4(3). [↑](#footnote-ref-50)
51. Rule 6 is expanded to include confirmation of the type of **biometric information** an agency holds in rule 6(1)(b). [↑](#footnote-ref-51)
52. Rule 10(1) proposes consideration of **privacy safeguards** and a proportionality assessment before commencing **biometric processing** of **biometric samples** that an agency holds (if not previously considered under rule 1). [↑](#footnote-ref-52)
53. Rule 11 proposes limiting the exception for disclosing biometric information if the source is a publicly available **biometric sample** sourced by means of **web scraping**. [↑](#footnote-ref-53)