

# DRAFT FOR CONSULTATION

New provisions are underlined

Deleted provisions are ~~struckthrough~~



This legislation is administered by the Office of the Privacy Commissioner. For more information please see:

Website: [www.privacy.org.nz](http://www.privacy.org.nz)

Contact phone: 0800 803 909

Contact address: PO Box 10094, Wellington 6140

## Biometric Processing Privacy Code 2020

This Code of Practice is made under section 32 of the Privacy Act 2020 by the Privacy Commissioner

### Contents

	Page
<b><u>Part 1</u></b> <b><u>Preliminary provisions</u></b>	
1	2
2	2
3	2
4	5
5	6

### Part 2 Biometric Processing Privacy Rules

6	Biometric Processing Privacy Rules	6
	Rule 1: Purpose of collection of biometric information	6
	Rule 2: Source of biometric sample	7
	Rule 3: Collection of information from individual <u>concerned</u>	8
	<u>Rule 3A: Collection of information other than from individual concerned</u>	9
	Rule 4: Manner of collection of biometric information	12
	Rule 5: Storage and security of biometric information	12

Rule 6: Access to biometric information	12
Rule 7: Correction of biometric information	13
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	13
Rule 9: Retention of biometric information	13
Rule 10: Limits on use of information	13
Rule 11: Limits on disclosure of biometric information	16
Rule 12: Disclosure of biometric information outside New Zealand	17
Rule 13: Unique identifiers	17

## Code of Practice

### Part 1 Preliminary provisions

#### 1 Title

This is the Biometric Processing Privacy Code 2025.

#### 2 Commencement

This code of practice comes into force—

- on 3 November 2025 for any type of biometric processing that has not commenced before that date; or
- on 3 August 2026 for any type of biometric processing that commenced on or before 3 November 2025.

#### 3 Interpretation

In this code of practice,—

**Act** means the Privacy Act 2020

**accessibility** means actions, measures, modifications or adjustments that help enable an individual with a disability a disabled individual to overcome or reduce barriers to participation on an equal basis with others

**adverse action** means, with respect to any particular individual, any action, informed by a result—

- to monitor or profile the individual; or
- that may adversely affect the individual's rights, benefits, privileges, obligations, or interests, including the imposition of a penalty or a fine; or
- that may cause loss, detriment, damage or injury to the individual; or
- that may result in humiliation, loss of dignity or injury to the feelings of the individual

**biological material** means—

- the whole or part of any organ, bone, tissue, or cell; or

- (b) blood or body fluids

**biometric categorisation** means an automated process of analysing biometric information—

- (a) to collect, obtain, create, infer or detect, or to attempt to collect, obtain, create, infer or detect health information, or personal information relating to an individual's—
  - (i) personality, mood, emotion, intention, or mental state; or
  - (ii) state of fatigue, alertness or attention level; or
- (b) to categorise the individual as part of a demographic category assigned to an individual on the basis of a biometric characteristic, such as the individual's sex, age, ethnicity or sexual orientation, including a demographic category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993;

but does not include—

- (c) the detection of a readily apparent expression; or
- (d) any analytical process that is integrated in a commercial service, including any consumer device, solely for the purposes of providing individuals with their health information, their personal information or an entertainment or immersive experience

**biometric characteristic** means—

- (a) a physical feature or quality of any part of an individual's body including their face, fingerprints, palmprints, iris, retina, voice or vein patterns; or
- (b) the way that an individual typically performs or responds to a task, action or decision with any part of their body, whether voluntarily or involuntarily, including the repeated motion or associated rhythmic timing or pressure of any part or feature of an individual's body such as the individual's gestures, gait, voice, heartbeat, eye movements, keystroke pattern, signature or handwriting style; or
- (c) a combination of any such distinctive attributes, including the way an individual sounds when they speak

**biometric identification** means the automated recognition of an individual's biometric characteristic for the purpose of identifying the individual by comparing the biometric characteristic with biometric information held in a biometric system

**biometric information** means personal information relating to a biometric characteristic for the purposes of biometric processing, such as—

- (a) a biometric sample; and
- (b) a biometric template;

but does not include any information about—

- (c) the individual's biological material;
- (d) the individual's genetic material;

- (e) the individual's brain activity; or
- (f) the individual's nervous system

**biometric processing** means the comparison or analysis of biometric information by a technological system, by means of any of the following—

- (a) biometric identification;
- (b) biometric verification; or
- (c) biometric categorisation

**biometric sample** means an analogue or digital record of an individual's biometric characteristic

**biometric system** means a technological system that is used for biometric processing

**biometric template** means a numerical or algorithmic representation of information extracted from a biometric sample

**biometric verification** means the automated one-to-one verification of an individual's claimed identity by comparing that individual's biometric information with biometric information held in a biometric system that has previously been associated with the individual

**disability** has the meaning in section 21(1)(h) of the Human Rights Act 1993

**health agency** has the meaning in the Health Information Privacy Code 2020

**health information** has the meaning in the Health Information Privacy Code 2020

**privacy risk** has the meaning in subclause (2)

**privacy safeguard** means an action, process or measure to reduce privacy risk

**protected rights** means the rights protected under the New Zealand Bill of Rights Act 1990

**readily apparent expression** 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

**result** means any personal information resulting from biometric processing, whether or not the result is accurate or inaccurate, false or misleading, undetermined or inconclusive, or a false positive or a false negative, and includes a candidate list or match, probable match or non-match, alert, prediction, analysis, assessment, decision, determination, recommendation, identification, score, calculation or inference about an individual

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

**technological system** means any computer system and its related devices and components (including any software, hardware, database, application, algorithm, sensor, camera or token), that calculates an outcome or controls a process, 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

**trial** means an agency carrying out biometric processing, for a trial period, for the purpose of providing the agency with information or evidence about the effectiveness of the biometric processing

**trial period** means a period that is no longer than is necessary to meet the objectives of the trial and that may include—

- (a) an initial trial period that is no longer than 6 months, and
- (b) if the objectives of the trial have not been met at the end of the initial period, one further trial period that is no longer than 6 months.

(2) In this code of practice, **privacy risk** is any reasonable likelihood that the privacy of individuals may be infringed, and includes any reasonable likelihood that—

- (a) an action relating to biometric processing may result in a breach of the protections for biometric information under the rules of this code of practice, such as the over-collection, over-retention or inaccuracy of biometric information, security vulnerabilities affecting biometric information, or a lack of transparency about biometric processing; (*breach of data protections*)
- (b) a result misidentifies or misclassifies an individual, including where the risk differs based on attributes such as the individual's race, ethnicity, gender, sex, age or disability (whether separately or in combination); (*bias*)
- (c) biometric processing for the purposes of surveillance, monitoring or profiling may result in any adverse action or deter an individual from exercising any protected rights; (*chilling effect*)
- (d) the purposes for which biometric information may be used or disclosed are expanded following the collection of the information, without the knowledge or authorisation of individuals; (*scope creep*) and
- (e) the ability of individuals to avoid monitoring is diminished in spaces where they may reasonably expect not to be monitored. (*surveillance*)

(3) A term or expression defined in section 7 of the Act and used, but not defined in this code of practice, has the same meaning as in the Act.

#### **4 Application of code of practice**

(1) This code of practice applies to:

- (a) the activity of biometric processing; and
- (b) biometric information as a class of information.

(2) This code of practice does not apply to the activity of biometric processing by a health agency, or to biometric information collected or held by a health agency, where the biometric information is health information.

(3) Rules 2, 3, 3A, 4(b) and 10(5) do not apply to an intelligence and security agency.

#### **5 Review of code of practice**

The Privacy Commissioner will undertake a review of this code of practice commencing no later than 3 November 2028.

## Part 2

### Biometric Processing Privacy Rules

#### **6 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**

- (1) Biometric information must not be collected by an agency unless, in the particular circumstances,—
  - (a) biometric processing is for a lawful purpose connected with a function or an activity of the agency; and
  - (b) biometric processing is necessary for that particular purpose, including—
    - (i) that biometric processing is effective in achieving the agency's lawful purpose; and
    - (ii) that the agency's lawful purpose cannot reasonably be achieved as effectively by an alternative means that has less privacy risk; and
  - (c) the agency has adopted and implemented such privacy safeguards as are reasonable in the circumstances; and
  - (d) the agency believes, on reasonable grounds, that the biometric processing is proportionate to the likely impacts on individuals.
  - (2) If, in the particular circumstances, an agency cannot comply with the requirements of subrule (1)(b) before collecting biometric information, the agency may establish a trial and defer compliance with that subrule until the end of the trial period.
  - (3) For purposes of subrule (1)(d), the agency must take into account the following factors—
    - (a) the scope, extent and degree of privacy risk from the biometric processing; and
    - (b) whether the benefit of achieving the agency's lawful purpose by means of biometric processing outweighs the privacy risk; and
    - (c) the cultural impacts and effects of biometric processing on Māori.
  - (4) For purposes of subrule (3), the benefit of an agency achieving its lawful purpose outweighs the privacy risk of biometric processing if, in the circumstances,—
    - (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.

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 2**  
**Source of biometric sample**

- (1) If an agency collects a biometric sample, 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,—
  - (a) that compliance would prejudice the interests of the individual concerned; or
  - (b) that compliance would prejudice the purposes of the collection; or
  - (c) that the individual concerned authorises collection of the information from someone else; or
  - (d) that the information is publicly available information; or
  - (e) 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
    - (v) to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual; or
  - (f) that compliance is not reasonably practicable in the circumstances of the particular case; or
  - (g) 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.

**Rule 3**  
**Collection of information from individual concerned**

- (1) If an agency collects biometric information from the individual concerned, the agency must take steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of the following—
  - (a) the fact that the information is being collected; and
  - (b) each specific purpose or purposes for which the information is being collected, specified with due particularity; and

- (c) whether there is any alternative option to biometric processing that is available to the individual in any particular circumstances; and
- (d) the intended recipients of the information; and
- (e) the name and address of—
  - (i) the agency that is collecting the information; and
  - (ii) the agency that will hold the information; and
- (f) if the collection, use or disclosure of the information is authorised or required by or under law—
  - (i) the particular law by or under which this is authorised or required, whether New Zealand law (including an authorised information sharing agreement), or the laws of another country; and
  - (ii) whether the supply of the information by the individual is voluntary or mandatory; and
- (g) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
- (h) the rights of access to, and correction of, information provided by rules 6 and 7; and
  - (i) a summary of the agency's retention period for biometric information; and
  - (j) the process (if any) available 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 of practice applies to; and
- (l) the location of where the agency's assessment under subrule 1(1)(d), or a summary of that assessment, is available to view, if publicly available, or whether the assessment or summary is available on request.

(2) Without limiting subrule (1), if the agency collects biometric information during a trial, the agency must take steps that are, in the circumstances reasonable, to ensure that the individual concerned is aware of the trial and the trial period.

(3) Where an agency is required to take steps to ensure the individual's awareness of the matters in subrules (1)(a), (b) and (c) and subrule (2)—

- (a) those steps must be taken before or at the time the biometric information is collected; and
- (b) information provided to the individual concerned—
  - (i) must be communicated in a manner that is clear and conspicuous; and
  - (ii) must include a location, address or other method enabling the individual to obtain further information about the biometric processing.

- (4) Any steps to ensure the individual's awareness of the other matters set out in subrule (1) 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.
- (5) An agency is not required to take the steps referred to in subrules (1) or (2) 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, and for the same purpose.
- (6) 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 or are reasonably in contemplation); or
  - (b) that compliance would prejudice the purposes of the collection;
  - (c) 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.

### **Rule 3A** **Collection of information other than from individual concerned**

- (1) If an agency collects biometric information about an individual other than from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of—
  - (a) the fact that the information has been collected; and
  - (b) each specific purpose or purposes for which the information has been collected, specified with due particularity; and
  - (c) whether there is any alternative option to biometric processing that is available to the individual in any particular circumstances; and
  - (d) the intended recipients of the information; and
  - (e) the name and address of—
    - (i) the agency that has collected the information; and
    - (ii) the agency that is holding the information; and
  - (f) if the collection, use or disclosure of the biometric information is authorised or required by or under the law, the particular law by or under which the collection

of the information is authorised or required, whether New Zealand law (including an authorised information sharing agreement), or the laws of another country; and

- (g) the rights of access to, and correction of, information provided by rules 6 and 7; and
- (h) a summary of the agency's retention period for biometric information; and
- (i) the process (if any) available 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
- (j) the right to complain to the Privacy Commissioner about any action that this code of practice applies to; and
- (k) the location of where the agency's assessment under subrule 1(1)(d), or a summary of that assessment, is available to view, if publicly available, or whether the assessment or summary is available on request.

(2) Without limiting subrule (1), if the agency indirectly collects biometric information during a trial, the agency must take steps that are, in the circumstances reasonable, to ensure that the individual concerned is aware of the trial and the trial period.

(3) Where an agency is required to take steps to ensure the individual's awareness of the matters in subrules (1)(a) and (b) and subrule (2)—

- (a) those steps must be taken before or at the time the biometric information is indirectly collected; and
- (b) information provided to the individual concerned—
  - (i) must be communicated in a manner that is clear and conspicuous; and
  - (ii) must include a location, address or other method enabling the individual to obtain further information about the biometric processing.

(4) Any steps to ensure the individual's awareness of the other matters set out in subrule (1) 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.

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

(6) 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; or
- (c) that compliance would cause a serious threat to—
  - (i) public health or safety; or
  - (ii) the health and safety of another individual; or
- (d) 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.

(7) It is not necessary for an agency to comply with subrules (1) or (2) if—

- (a) the agency collects biometric information for the purpose of determining whether the information is of enduring value for general public interest and should be archived for public reference, study, or exhibition; and
- (b) compliance is likely to seriously impair the agency's achievement of the purpose in subrule (7)(a).

(8) It is not necessary for an agency to comply with subrules (1) or (2) if compliance would be likely to prejudice—

- (a) the security or defence of New Zealand, the Cook Islands, Niue, Tokelau, or the Ross Dependency; or
- (b) the international relations of the Government of New Zealand, the Cook Islands, or Niue; or
- (c) the relations between any of the Governments of—
  - (i) New Zealand; or
  - (ii) the Cook Islands; or
  - (iii) Niue; or
- (d) the entrusting of information to the Government of New Zealand on a basis of confidence by—
  - (i) the Government of any other country or any agency of the Government of any other country; or
  - (ii) any international organisation.

(9) It is not necessary for an agency to comply with subrules (1) or (2) if compliance would—

- (a) disclose a trade secret; or
- (b) be likely to unreasonably prejudice the commercial position of—
  - (i) the person who supplied the information; or
  - (ii) the individual concerned.

(10) Rule 3A does not apply to biometric information collected by an agency—

- (a) before 1 May 2026 in respect of any type of biometric processing by that agency that commenced after 3 November 2025; or
- (b) before 3 August 2026 in respect of any type of biometric processing by that agency that commenced after 3 November 2025.

#### **Rule 4**

#### **Manner of collection of biometric information**

An agency may collect biometric information only—

- (a) by a lawful means; and
- (b) by a means that, in the circumstances of the case (particularly in circumstances where information is being collected from children or young persons),—
  - (i) is fair; and
  - (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

#### **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 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 6**

#### **Access to biometric information**

- (1) An individual is entitled to receive from an agency upon request—
  - (a) confirmation of whether the agency holds any biometric information about them; and
  - (b) confirmation of the type of biometric information the agency holds about them; and
  - (c) access to their biometric information.
- (2) If an individual concerned is given access to biometric information, the individual must be advised that, under rule 7, the individual may request the correction of that information.

(3) This rule is subject to the provisions of [Part 4](#) 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—

- (a) provide the agency with a statement of the correction sought to the information (a **statement of correction**); and
- (b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought.

(4) 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.

(5) If an agency corrects biometric information or attaches a statement of correction to biometric information, that agency must, so far as reasonably practicable, inform every other person to whom the agency has disclosed the information.

(6) Subrules (1) to (4) are subject to the provisions of [Part 4](#) 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 information**

#### *Limits on use of information for biometric processing*

(1) If an agency holds personal information that was not collected in accordance with rule 1, the agency must not use the information for biometric processing, nor may an agency

that holds biometric information for the purposes of any type of biometric processing, use the information for another type of biometric processing.

- (2) It is not necessary to comply with subrule (1) if, in the particular circumstances—
  - (a) the biometric processing is necessary in achieving the agency's lawful purpose for which the information was obtained, including—
    - (i) that biometric processing is effective in achieving the agency's lawful purpose; and
    - (ii) that the agency's lawful purpose cannot reasonably be achieved as effectively by an alternative means to biometric processing, or by an alternative type of biometric processing, that has less privacy risk; and
  - (b) the agency has adopted and implemented such privacy safeguards as are reasonable in the circumstances; and
  - (c) the agency believes, on reasonable grounds, that the biometric processing is proportionate to the likely impacts on individuals.
- (3) If, in the particular circumstances, an agency cannot comply with the requirements of subrule (2)(a), the agency may establish a trial and defer compliance with that subrule until the end of the trial period.
- (4) For purposes of subrule (2)(c), the agency must take into account the relevant factors in rule 1(3).

*Limits on use for biometric categorisation*

- (5) An agency that holds biometric information must not use that information for biometric categorisation unless subrule (6), (7), (8) or (9) applies.
- (6) This subrule applies if the use of biometric information is to categorise the individual concerned on the basis of their age, or any demographic category that is not a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993.
- (7) This subrule applies if, in the circumstances of the case, the agency believes, on reasonable grounds,—
  - (a) that the use of biometric information is necessary to assist an individual with accessibility; or
  - (b) that the use of biometric 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
  - (c) that the biometric information is to be used for statistical or research purposes, subject to ethical oversight and approval, and will not be published in a form that could reasonably be expected to identify the individual concerned.
- (8) This subrule applies if—
  - (a) the use of biometric information is to obtain, infer, detect or to attempt to obtain, infer or detect personal information about the individual's state of fatigue, alertness or attention level; and

- (b) the agency believes, on reasonable grounds, that the use is necessary to prevent or lessen a risk to—
  - (i) public health or public safety; or
  - (ii) the life or health of the individual concerned or another individual.
- (9) This subrule applies if—
  - (a) the use of the individual's biometric information is to obtain, infer, detect or to attempt to obtain, infer or detect health information; and
  - (b) the agency believes, on reasonable grounds, that the use is expressly authorised by the individual concerned.

*Other limits on use of biometric information*

- (10) Without limiting subrule (1) or (5), 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.

(11) In addition to the uses authorised by subrule (10) 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**

(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,—

- (a) 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
- (b) that the disclosure is to the individual concerned; or
- (c) that the disclosure 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 disclose the information; or
- (e) 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
- (f) 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
- (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or
- (h) 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

- (i) 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—
  - (a) 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 the Act, as modified by this code of practice; or
  - (b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to the Act, as modified by this code of practice; or
  - (c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in the Act, as modified by this code of practice; or
  - (d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or
  - (e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country and the disclosure is not precluded by any limitation or qualification prescribed in respect of that country under section 214 of the Act; or
  - (f) 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 the Act, as modified by this code of practice (for example, pursuant to an agreement entered into between A and B).
- (2) 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).
- (3) In this rule,—
  - prescribed binding scheme** means a binding scheme specified in regulations made under section 213 of the Act.
  - prescribed country** means a country specified in regulations made under section 214 of the Act.

### **Rule 13** **Unique identifiers**

- (1) An agency (A) may assign a unique identifier that is a biometric template 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 that, to A's knowledge, is the same unique identifier that has been assigned to that individual by another agency (B), unless—
  - (a) A and B are associated persons within the meaning of [subpart YB](#) of the Income Tax Act 2007; or
  - (b) the unique identifier is to be used by A for statistical or research purposes and no other purpose.
- (3) 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.
- (4) A must take any steps that are, in the circumstances, reasonable to ensure that—
  - (a) a unique identifier is assigned only to any individual whose identity is clearly established; and
  - (b) 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).
- (5) 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.