New Zealand Banking Association
Te Rangapū Pēke

# Submission

to the

# Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu

on the

# Exposure draft of a biometric processing code of practice: consultation paper

22 May 2024

**NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE**
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

Classification: PROTECTED

## About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following eighteen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - KB Kookmin Bank Auckland Branch
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

## Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Associate Director, Policy & Legal Counsel
sam.schuyt@nzba.org.nz



Classification: PROTECTED

## Introduction

4. NZBA welcomes the opportunity to provide feedback to the Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu (**OPC**) on its exposure draft of a biometric processing code of practice: consultation paper (**Consultation**) and draft Code of Practice (**Code**). NZBA commends the work that has gone into developing this document and the technical analysis supporting it.

5. We are, in principle, not opposed to the introduction of protections in relation to biometric processing. We do however have some concerns with the Code as currently drafted. There is a balance to be worked through in the Code between customer expectations of services, business needs to provide services in a digital and modern world, and privacy protections. NZBA is concerned that the current draft Code goes too far and so fails to strike the right balance.

6. This submission contains detailed feedback on the overall Code, as well as specific responses to certain definitions (Appendix 1) and consultation questions (Appendix 2). In summary:

    6.1. We are concerned that the definitions provided in the draft Code are overly technical and complex, making interpretation and application of the Code difficult (for example in relation to the definition of biometric information which is too broad).

    6.2. We strongly oppose any retrospective application of the Code and suggest that OPC consider further transitional arrangements.

    6.3. The exceptions under rule 4(3) should be expanded to include an exception for fraud detection and prevention solutions.

    6.4. Transparency provisions in the Code should remain consistent with the current approach under IPP3.

    6.5. We agree with the need for "privacy safeguards" and for the flexibility in approach that has been provided for in the draft Code, but submit that further clarity is needed on the test for reasonableness (in particular, that when deciding which factors to apply, the proportionality assessment must be taken into account).

    6.6. In our view, a narrower application would still be a helpful step forward in introducing biometric protections while also being achievable in terms of implementation. OPC could then consider whether to expand the Code in time, and consult further at that stage.

## Scope

<u>Definitions</u>

7. NZBA considers that some key definitions are too broad and that this will make the Code complex and challenging to implement. The Code would, in our view, still be effective with a narrower application, as expanded upon below.

8. We also consider that the meaning of some definitions is unclear and strongly recommend that these are clarified, particularly given that there will be different risk



Classification: PROTECTED

levels associated with each. For example, it is unclear whether "face" refers purely to that captured in CCTV, or on a passport, or on a device used to unlock a phone where the provider does not have access to the original facial record.

9. Some definitions have been significantly altered since the previous consultation draft. Some are missing detail, appear complex, very scientific and definitions are overlapping. This has made them hard to follow and their application seems very unclear.

10. We submit that worked examples would help ensure that definitions are being correctly understood and the Code is correctly applied.

11. We have provided our views below on two significant examples of our concerns with definitions. Further feedback on the defined terms used in the Code is set out in Appendix 1.

*Biometric Information*

12. NZBA submits that the definition of biometric information (and within this, definitions of behavioural and physiological biometrics) is too broad.

13. Traditionally in New Zealand law, biometrics has meant face, iris/retina, and fingerprints /palm prints/ footprints. The Code takes this much broader in line with some other jurisdictions (in particular, the EU) including some things which, in a bank's current systems, would be difficult to track or attribute as a biometric to an individual, particularly retrospectively as the Code proposes.

    13.1. For example, signatures, handwriting style and pattern of using a digital device being included in the definition of a behavioural biometric is very broad and will, practically, be quite difficult to implement for a typical bank's existing data. Signatures are commonly used by banks as contract acceptance as well as identity verification, and there is movement towards machine-based signature verification.

    13.2. Considered against the proposed retrospective application of the Code, the resultant effect could be that banks need to recollect customers' signatures once the Code comes into effect.

    13.3. Consideration must also be given to s 228 of the Contract and Commercial Law Act 2017, which already provides for reliability of signature. Without the removal of signatures and handwriting style from the definition, this risks potential harm to customers as well as wide-scale disruption, and inconvenience to customers and current banking processes across the industry.

    13.4. We therefore submit that OPC should consider the follow-on effects of capturing signatures, and if it does retain them, that an exception is added to enable banks to automatically verify signatures.

14. We note that the Code only applies to automated processing in its current draft which may minimise the impact on retrospective data, but it would still have impacts on future technology initiatives by businesses including banks.



Classification: PROTECTED

15. In our view, the scope of the definition of 'behavioural biometric' should be amended to remove signatures and handwriting style. Narrowing the scope of the definition would, we submit, still result in a Code which is effective – but it would also, importantly, be appropriately balanced and would introduce biometric protections at the right pace and result in a more achievable and successful implementation.

16. Further, there are in our view benefits in using voice analytics to survey individuals' responses or review calls when they have called a contact centre, or to verify their identity when they call a bank. This helps ensure customers are getting the right services, have received the right outcome and are happy with the outcome, and for businesses to be sure they are speaking to the right person. We submit that the Code should allow for this use of voice analytics, and that it should be drafted carefully to avoid inadvertently restricting the use of voice biometrics.

*Privacy Risk*

17. NZBA also has some concerns about the Code's proposed definition of privacy risk. In our view, how to define such risks and the appropriate safeguards would sit more naturally with organisations and we question why the definition is therefore part of the Code.

18. We submit that, alternatively, OPC could offer guidance on how to approach privacy risk for biometrics rather than have a definition in the Code itself.

19. As to the risks that are listed, NZBA is particularly interested in what is expected from risk (vi): *the individual is not aware of the collection of biometric information or does not understand the purposes of biometric processing; (lack of transparency).*

20. It is difficult to track or find out what a customer knows or understands, this is very difficult to measure – particularly when OPC has publicly said that agencies need to do more than just have a privacy statement on their website or a tick-box to confirm that someone has read and understood the privacy policy or T&Cs.

21. If this risk is to be retained, further guidance and clarity would be welcomed to indicate what reasonable steps an agency may take to mitigate this risk.

<u>Automated processing</u>

22. NZBA welcomes the reduction in scope to include 'automated processing' only. However, we believe that the corresponding definitions, such as "biometric processing" and "biometric systems" should be limited to instances where the system involves no human input, assistance or oversight.

23. We are concerned that processing that is largely or almost wholly manual will now also fall within the Code's scope (i.e. regardless of extent). We believe that the Privacy Act should solely apply to the governance of manual processing of biometric information.

24. If aspects of manual processing find their way into the Code's scope, we believe large-scale uplift (and disruption) would be needed to our members' current customer due diligence processes, and their storing of photos and videos.



Classification: PROTECTED

Fair processing limits – inner state

25. We submit that the proposed rule 4 has gone too far. While the processing of biometrics to infer or attempt to infer emotions, personality or mental state does not apply to the banking industry, we find the definition of "inner state" broad and open to subjective interpretation.

26. Given the removal of the restriction on marketing, we assume it is intended to canvass any potential privacy risk with this activity. The effect of the proposed limitations will be that very little biometric information collection is permitted with one main exception, biometric identification. Broadly speaking, we are concerned that the revised language in the Code no longer strikes an appropriate balance between privacy protections and the OPC's original intention to "preserve the benefits of using biometric information and technologies and allow for continued innovation".

27. We appreciate that removing the restrictions entirely may create a risk that some agencies use data in an attempt to detect moods and emotions. However, we submit that the current definition, including "intention" and "mental state", is very broad and should be narrowed – for example, by limiting it to inferring or attempting to infer an individual's religious or political views, ethnicity, or sexual orientation (i.e. the generally accepted classes of "sensitive information").

28. The availability and lawful use of biometric technology is crucial to the banking sector as a whole, and to end-customers going forward. At a time in which current fraud prevention and detection efforts are struggling to keep pace with increasingly complex methods of fraud perpetrators, biometric technology offers a means to help provide our customers with secure access to banking products using methods that are convenient, efficient and reasonably safe. It is important that the limitations on fair processing cater for this context.

29. On the whole, we prefer the IPP4 principles-based approach, which is left to be applied, case by case, by each agency.

Fair processing limits – physical state

30. In line with our comments at paragraph 25 above, we believe that in terms of physical state the proposed rule 4 has also gone too far. The definition of physical state is too broad and is open to wide subjective interpretation.

31. The effect of the proposed limitations will be that very little biometric information collection is permitted with one main exception, biometric identification. We do not agree with the fair processing limit to using biometrics to detect 'physical state' generally.

32. We prefer the IPP4 principles-based approach, which can be applied, case by case, in the manner determined by each agency. Agencies should be permitted to process this type of information if they have reasonable grounds to believe it is proportionate – this aligns with the OPC's objective of continued innovation as noted in the previous OPC discussion paper.

33. There may be good reasons to collect this information, such as fraud prevention and detection. Agencies should be permitted to collect the information if they undertake the proportionality assessment required under new rule 1 and conclude that the biometric processing is not disproportionate. While we agree the collection of biometrics for the



Classification: PROTECTED

purposes of inferring an individual's physical state may increase privacy risks in some scenarios (e.g. monitoring whether user is paying attention to an advertisement), there are other benefits associated with the collection of such data (e.g. fraud prevention and detection).

34. For example, agencies should be permitted to classify individuals' behavioural biometric information (such as collecting information about mouse movement, which may demonstrate the individual's attention level which may also indicate an individual's physical state) where the collection is proportionate. For that purpose, we recommend expanding the list of exceptions in rule 4(3) to include fraud prevention and detection.

35. This allows a proactive prevention approach which is in our view the best way to manage fraud risk, as opposed to rule 4(3)(d)'s reactive prevention approach. We consider it may be too unclear to determine the extent of where a bank owes a customer a "duty of care" and it is preferable to simply refer to an express fraud prevention and detection exception instead. Agencies would be required to determine the collection is proportionate.

36. We submit that biometric processing of age information should be permissible if an agency is satisfied that is proportionate. There may be good reasons to collect this information, such as fraud prevention and detection. Agencies should be permitted to collect the information if they undertake the proportionality assessment required under new rule 1 and conclude that the biometric processing is not disproportionate.

<u>Retrospective application</u>

37. In principle, NZBA opposes any retrospective application of the Code.

38. We expect there will be a significant compliance burden, cost and technical complexity if applying any potential roll-back in the banking sector, particularly because many banks would have relied on third party service providers and taken steps to ensure it has met its existing privacy obligations (including notice requirements). It is also unclear how this would work in practice given already existing arrangements addressing earlier customer fraud/scam losses. We are concerned that it could result in confusion and frustration to millions of banking customers.

39. The OPC should, therefore, consider the following potential additional transitional arrangements:

    39.1. Grandfather existing arrangements of biometric information.

    39.2. Allow existing uses of biometric information that were collected before the implementation of any new Code to continue under the current Privacy Act regime.

    39.3. Establish a clear cutoff date after which new practices under any new Code will apply to all biometric information processing activities.

    39.4. Consider phased implementation such as introducing the new Code in phases, prioritising high-risk or high-impact uses of biometric information first, providing a timeline for different sectors or use cases to come into compliance with a Code gradually.



Classification: PROTECTED

40. If retrospective application is required, we submit that 6 months is too short a timeframe and that a transitional period of at least 12 months would, in our view, be more appropriate.

41. Additionally, it should be possible for an agency to obtain an extension to this 12-month timeframe, where they are unable to comply within this transitional period because of the complexity of making necessary adjustments to processes, notification requirements (if required) and systems (with third party providers and technology changes often involved, and given implementing certain privacy safeguards may also take longer than others) without penalties.

## Proportionality

42. We support, in principle, the requirement of undertaking proportionality assessments. However, we believe that agencies should be permitted to undertake their assessments based on their own internal processes.

43. Our preference is for privacy impact assessments (**PIA**s), with their proportionality assessments, to be carried out by agencies, but for them to remain internal confidential documents. Agencies should be encouraged to undertake rigorous and robust internal analysis about privacy issues without fear that these assessments might be mandatorily published.

44. For a PIA process to be meaningful and to address the commercial considerations of a business, it must be able to be done in a full and frank way. The threat of external publication will prevent the process addressing any confidential, privileged, or commercially sensitive information (such as reveal the solution design, internal processes, risk controls and intellectual property).

45. Therefore, agencies should be able to choose themselves whether they wish to publish their PIA, dependent on the circumstances. This means that further clarity is required to explain how agencies can "demonstrate that their biometric processing is proportionate"[1] to comply, while still maintaining the required level of confidentiality.

46. We further submit that agencies should be allowed a longer time to complete assessments for existing biometric systems or providers, but not necessarily for new systems. Allowing for a year for existing systems would in our view be preferable.

47. In relation to the six factors listed in rule 1(2), we note there is a requirement to take into account not only cultural impacts on Māori when carrying out the rule 1 proportionality assessment, but also the cultural impacts on any NZ demographic group. This language is undefined and very broad and is likely to be unworkable.

48. In practice, considering the cultural impacts or effects of the biometric processing on Māori and other demographic groups could be difficult – for example, how will agencies know whether they have sufficiently "demonstrated that they have thought about these factors and can point to reasons why they think it is proportionate" to proceed with biometric processing?

49. We submit that further clarity (preferably by way of additional guidance) is required on how agencies can demonstrate they have thought about these factors. Our preference

[1] At page 25 of the Consultation.



Classification: PROTECTED

is for this assessment to be performed as part of an agency's business as usual internal process, pursuant to the PIA, and for it to remain confidential to that agency.

## Privacy Safeguards

50. We agree with the requirement for agencies to adopt privacy safeguards that are reasonable in the circumstances (rule 1(c)). In particular, we welcome and endorse the approach of consent not being mandatory as it will not always be practical and relevant to do so especially across online digital banking channels. The Privacy Act also does not require it.

51. Current IPP3 requirements are to ensure awareness via the relevant terms and conditions that incorporate and link to the relevant bank's privacy statement. Currently, where there are updates to these privacy statements, public notice type 'awareness' updates are then published, and the degree of public notice given depends on the materiality of the change.

52. The additional transparency requirements in the draft Code (conspicuous notice and accessible notice) would require further "awareness" of the fact and purposes of biometric processing without the need for express consent.

53. A requirement for express consent for the collection of all biometric information covered by the Code could have a significant detrimental impact on businesses throughout Aotearoa New Zealand – and may in some instances be unachievable (for example in relation to costs and system changes).

54. There may be significant compliance costs involved for organisations with a large customer base to implement and manage express consent. While we agree authorisation is an appropriate privacy safeguard, the test for reasonableness should have a higher threshold, taking into account the proportionality assessment of privacy risks and benefits.

55. The main use case for collecting biometric information in the banking sector is currently fraud and criminal activity prevention and detection (including identity verification). We believe that this benefits customers and has a strong public interest component given the current environment where fraud and criminal activity is increasing, and will continue to increase, at pace. Apart from the Privacy Act not requiring express consent, the main arguments against express consent in the fraud prevention and detection area are as follows:

    55.1. Fraudsters would simply decline requests to consent this information, which would undermine the efficacy of proposed fraud prevention and detection solutions and continue to expose our customers to online fraud and scams.

    55.2. By requiring express consent to collect biometric information for these fraud prevention and detection purposes, the concern is that some customers would decide not to consent. This could result in them being at higher risk of fraud occurring, i.e. in a banking context, those customers would be required to bank using other (non-digital) banking channels. It is also in line with IPP5 for financial service providers to be able to take such security safeguards as are reasonable in the circumstances against loss, access, use, modification, or disclosure that is not authorised, and other misuse to protect the personal information of our customers. Collecting biometric information within digital banking channels helps improve the security posture of those channels, and



Classification: PROTECTED

therefore helps protect our customers' information and assets within those channels.

55.3. The technical complexity of these solutions and particularly the complexity of rolling out a consent mechanism for trust accounts, joint accounts and vulnerable customers such as children or the elderly.

56. We support the Code providing the autonomy for agencies to implement appropriate privacy safeguards as are reasonable in the circumstances to both ensure privacy risk is adequately addressed but also to meet the need to achieve our business objectives efficiently. In our view, the test for reasonableness should have a higher threshold, taking into account the proportionality assessment of privacy risks and benefits.

We agree with the definition of "privacy safeguards" and agree the list of safeguards are appropriate for mitigating privacy risks. However, the Code concept of "relevance" is difficult to apply as currently drafted and ideally would need further guidance and examples to be understood.

## Biometric Watchlist Concerns

57. NZBA supports the intent of a "biometric watchlist" as provided for in the last consultation, where a watchlist captures problem gamblers, or individuals who have been trespassed for violence, threats or criminal activities.

58. We are however concerned that the Code requirements relating to a "biometric watchlist" would impede banks deploying fraud prevention and detection software to protect customers and the public. Banks are currently receiving heightened feedback and direction from Government, the Banking Ombudsman and other regulators and consumer bodies such as Consumer NZ to take increasing steps to prevent and detect fraud and other financial crime. Therefore, it is critical that fraud prevention and detection software is not caught by this privacy safeguard. We consider the current scope of this concept has therefore gone too far and should be narrowed.

59. The effect of the "biometric watchlist" safeguard as provided for in clause 3(b) of the Code is extremely broad, and could be difficult for banks to implement, in particular for fraud prevention. For example, a requirement to advise the individual if an adverse action will be taken may alert the fraudster. A requirement to alert the individual concerned may also risk an agency breaching its 'tipping off' obligations under the Anti-Money Laundering / Counter Financing of Terrorism Act 2009.

60. We would also propose an additional fraud prevention and detection exception be built into rule 4(3) to cater for these scenarios, which have both individual and public benefits.

61. We query the 'trained human oversight' safeguard. This is specific to monitoring, recording and correction of flawed biometric results. Consideration may be given to also include biometric systems, e.g. monitoring and correction of flawed algorithms in biometric systems.

## Notification / Transparency

62. NZBA submits that current IPP3 obligations are sufficient and that the proposed new rule 3 requires more detail than is reasonable in the circumstances. To the extent that



Classification: PROTECTED

OPC is intent on including the conspicuous / accessible notice requirements, the following specific points should be considered.

62.1. We submit that rule 3(1)(b) requires clarification, as it is currently unclear what is meant by “specified with due particularity”.

62.2. We further submit that the requirement to provide individuals with a summary of the agency’s retention policy for biometric information should be omitted. As per the definition in the draft Code, “biometric information” includes “behavioural biometric, physiological biometric, biometric sample, biometric template and biometric results”. These may require different retention periods given the different purposes they might be used for, particularly in highly regulated industries such as financial services. Providing a copy of our retention policy is likely to create additional confusion for individuals. We believe IPP9, in conjunction with rule 9 (where agencies cannot retain personal information for longer than necessary) already provides sufficient protection.

62.3. Similarly, the requirement to provide individuals with a list of the agency’s policies, protocols and procedures should also be omitted. These documents would ordinarily be confidential and commercially sensitive. Also, the requirement to provide a “list of document names” should also be omitted as this list would not provide individuals with any further context to how their biometrics are being processed.

Conspicuous Notice

63. It is unclear to us whether:

63.1. the OPC also expects the matters in rule 3(1) to be covered in an agency’s privacy statement.

63.2. the exception in rule 3(7) relating to a recent previous occasion also applies to the conspicuous notice under 2(b).

63.3. a combined statement (i.e. a privacy statement and biometrics privacy statement in a single document) would be sufficient.

63.4. an agency must notify that no alternatives to biometrics exist.

64. We are concerned that conspicuous notice might be required each time the information is collected (i.e. at each log in). This is different to the current IPP3 requirement and the Code requirement regarding accessible notices. In both cases, further notice isn’t required where it has been provided on a recent previous occasion.

65. If a requirement for repeated notices requires a pop-up notification each time a user logs in to their banking app or internet banking, we are concerned that this would create a negative customer experience, reducing the impact of the relevant notice and going against industry trends. Many of our members’ users log on to their banking apps several times a day. Repeated notices can result in potential notification fatigue, with potential risks around users dismissing the notifications without fully reading them.



Classification: PROTECTED

66. Additionally, we do not believe that requiring conspicuous notice every time a user logs on increases awareness or understanding of the type of biometric processing that is taking place.

67. If the OPC is intent on regular presentation of the conspicuous notice, we propose that the conspicuous notice should be presented to users at a frequency that is proportionate to the risk of the biometric processing or if there is a material change in the types of biometric data collected, used or disclosed. We would suggest that twelve months are allowed for low-risk biometric processing, and there may be circumstances where the presentation of the conspicuous notice solely at the outset of the use is both sufficient and appropriate, i.e. where a user actively accepts the conspicuous notice's terms before continuing and the particulars of the collection and use of biometric information remain unchanged following such agreement.

Accessible Notice

68. NZBA submits that the notification and transparency requirements for accessible notices are unnecessarily onerous. Under the Code, an "accessible notice" must be independent of any privacy statement, yet the information required in the notice under rule 3(1) duplicates a lot of the details typically presented in a privacy statement.

69. In our view, a more straightforward approach would be for consumers to refer to one overarching privacy statement, rather than have to read and understand two separate statements.

70. In terms of the information required under the accessible notice, our preference is to keep the required notification at a similar level to the current IPP3 notice level / requirements where the agency can determine the steps required, in conjunction with considering what is reasonable in the circumstances, particularly where there are less sensitive use cases such as the collection of behavioural biometric information.

71. We are concerned that for technical rollouts for automated processing of biometric information pan-bank, the IPP3 content suggested by the draft Code is too detailed and prescriptive and will lead to customer notification fatigue, customer confusion and apprehension. We consider that with particularly large systematic changes this type of detailed notification is unlikely to assist consumers either in the form it is presented or in the accuracy. In some instances, aspects of specific arrangements may generate inaccuracies in the notification (for example, the maximum duration for which the biometric information would be retained may not be known at the commencement of a development).

72. Our view is that transparency should remain dealt with in line with the current IPP3. Agencies can then self-determine what are "reasonable" steps to take to make individuals "aware" of the prescribed factors in the circumstances.

73. To the extent OPC may still be intent on this approach, we submit that certain clauses in rule 3(1) should be optional and agencies should have the autonomy to decide whether or not to include these in their accessible notice. For example, the summary of a retention policy (i) and a list of agency's policies, protocols and procedures (m) should not be required. This is contrary to the approach of many other financial service regulators. As a pragmatic solution, agencies should be able to link to their accessible notice to their current privacy statement.



Classification: PROTECTED

Exceptions to notification

74. We agree with the exceptions and do not believe that anything should be removed. However, as noted above, we are of the view that the exception in rule 3(7) relating to a recent previous occasion should also apply to the conspicuous notice under 2(b).

75. We submit that it would be helpful for OPC to provide examples around when an agency may believe on reasonable grounds that non-compliance would prejudice the purposes of collection. For example, where the sole purpose of collection is to detect and prevent fraud and criminal activity, in our view, providing the conspicuous and detailed accessible notice may tip-off the scammers and fraudsters and essentially defeat the specific purpose of the collection of the information.

**Further comments**

76. NZBA is supportive of some general exceptions to the Code for privacy reasons outside of the Biometrics Code. This is particularly important for vulnerable customers: where a bank has genuine concerns about that customer, they may benefit from having their information disclosed to other agencies.

77. We would also appreciate further clarification / guidance on:

    77.1. Platforms that have their own existing privacy obligations – for example, if large international platforms have existing privacy obligations and those platforms comply with those obligations, but may have some differences to the Code, what would an agency need to do to use those systems?

    77.2. In relation to rule 12 and the disclosure of biometrics outside of New Zealand, would there be an exception consistent with IPP12 where "the personal information is sent to an agent for storage or processing and the agent does not use or disclose the information for its own purposes" (where in this case there is no "disclosure" for the purposes of the Act)?

    77.3. Further, we would appreciate clarification on whether biometric information that has been anonymised, encrypted and unable to be traced back to an identifiable individual at the time of disclosure would be excluded from rule 12.



Classification: PROTECTED

New Zealand Banking Association
Te Rangapū Pēke

**APPENDIX 1: Feedback on definitions**

| Definition | Comments |
|---|---|
| **Behavioural biometric** | Peoples' signatures are commonly used to authorise payments and other instructions at bank branches, or online using platforms such as eSign. Currently, these signatures are usually processed entirely manually and would, therefore, not be subject to the biometric processing requirements of the Code. However, this situation seems likely to change, as banks and other agencies move towards machine-based signature verification (i.e. banks and AI generated signature check customer documentation). We therefore strongly recommend that an exception is added to enable banks and agencies to automatically verify signatures and for that to be outside the scope of the Code. |
| **Biometric processing, biometric verification and identification** | These definitions should be simplified. While we agree that "biometric search" means you compare a particular data point against a database of data to verify or identify, the current drafting requires the reader to go to three to four different definitions to understand what "biometric verification" and "biometric identification" also mean. Worked examples should also be provided in the accompanying guidance to help agencies apply the Code.<br><br>As currently drafted, the overarching technical complexity of the Code appears to make it inaccessible for both organisations and individuals to interpret and apply. |
| **Biometric search, query, reference, sample, template and comparison decision** | The technical definitions have created an overly complex and technical approach, with a layering of definitions within definitions. For example:<br>• "biometric search" means the action of comparing a biometric query with one or more biometric references to make a comparison decision; and<br>• "biometric query" means a biometric sample or a biometric template that is used as an input in a biometric search.<br><br>There are 14 different derivative definitions of the term "biometric" now included.<br><br>We are concerned that it will be too hard for organisations and individuals to interpret and apply the Code. We can foresee that additional OPC guidance will be required to make sense of the definitions. |

| Definition | Comments |
|---|---|
| **Biometric classification** | While we agree with the intent to exclude some processes from the definition, a number of the definitions are confusing and need to be simplified.<br>For example:<br>• the exception to the definition of “biometric classification” is confusing and difficult to apply;<br>• it is unclear what the following words permit: “the effect of the integration does not circumvent the rules in the code”; and<br>• it is difficult to understand which types of products, with some form of “biometric classification” built in, would/would not be in scope of the exception.<br>Worked examples might also help agencies better apply the Code. |
| **Benefit** | We agree with the definition of “benefit” and support the OPC’s view that fraud detection is considered as a benefit for agencies.<br>We agree that higher weighting should be given to public and individual benefit than the arising privacy risk. |
| **Privacy safeguards** | We agree with the definition of “privacy safeguards” and agree the list of safeguards are appropriate for mitigating privacy risks. However, the Code concept of “relevance” is difficult to apply. Examples would be required.<br>We support that individual authorisation (noting that there is no current definition of authorisation” and based on OPC approach to date, includes both implied and express authorisation) is one of the safeguards and endorse that it is not a mandatory requirement for biometric processing. |

**APPENDIX 2: Responses to specific consultation questions**

| Question | Response |
|---|---|
| **Q1:** Do you agree with these provisions? Do these rules or considerations adequately respond to concerns about Māori data? Do you have any suggestions for changing them? Have we missed anything? | Given the complexity of Māori data, we agree that it would be near-impossible in most cases for agencies to distinguish between Māori and non-Māori biometric information, unless it was tied to information about the ethnicity of an individual. Our members do not typically collect ethnicity information. |
| **Q23:** Do you agree with the matters that need to be on the conspicuous notice? Are there any items that you think should be added the conspicuous notice? Or removed? | If the OPC is intent on the conspicuous notice approach, we agree with the matters that need to be in the conspicuous notice.<br><br>However, we seek clarity on rule 3(1)(b), what is meant by "specified with due particularity"? For some digital channels within the banking industry, we may have limited space to convey such matters and this may contribute to customer notification fatigue. |
| **Q31:** Do you agree with the fair processing limit on using biometrics to place people in categories that are protected under the HRA? Are there any categories we've missed that are intrusive? Can you think of any beneficial uses for placing people into these categories? | We agree with the limit on using biometrics to place people in categories that are protected under the HRA.<br><br>However as noted in Q32, biometric processing of age information should be permissible if it is proportionate. |
| **Q32:** Do you agree with the exception for age-estimation? Do you agree with the way we've drafted the age-estimation exception – can only use it if necessary to comply with lawful obligation to apply an access limit or meet a duty of care? | We agree with the exception for age-estimation, however, we recommend that the exceptions under rule 4(3) be expanded to specifically include fraud prevention (or other benefits for the public or individuals as identified under the proportionality test). For example, biometric fraud detection tools may |

| Question | Response |
|---|---|
| | detect a difference between the account owner's age and the user's (fraudster's) age. In this case, the exception would protect the account owner. This exception could also provide additional benefits for more vulnerable customers such as the elderly and should be permitted when the collection is proportionate. |
| **Q33:** Do you agree with providing the standard 'serious threat' and 'research' exceptions to the fair processing limits? Do you agree that the research exception should be strengthened by adding written authorisation requirement and ethical oversight and approval requirements? | We agree with the standard serious threat and research exceptions. |
| **Q34:** Do you agree with the exception to the fair processing limits for assisting an individual with accessibility? Do you agree with our definition of accessibility? | We agree with the assisting an individual with accessibility exception. |
| **Q35:** Do you think there needs to be other exceptions to the fair processing limits? What exceptions would you suggest and why are they needed? | We suggest exceptions to also apply to biometric processing that is used to protect individuals against physical, mental and monetary harm (such as fraud). This allows a proactive prevention approach which is the best way to manage fraud risk, as opposed to rule 4(3)(d)'s reactive prevention approach.<br><br>Agencies would be required to determine the collection is proportionate. |