LexisNexis® | *Regulatory Compliance*

Diligent

The Biometric Shift: New Zealand's Path to Ethical Data Stewardship

Contents

Introduction

In this digital age, faces, fingerprints, and voices are not merely personal and identifying characteristics, but are also means by which we access services, identity protection, and our relationship with emerging technologies. Although these are useful tools, they also present a considerable risk when left unmanaged. Recognising the dual use of biometric technologies, with the potential for both use and misuse, the Office of the Privacy Commissioner (OPC) published a final version of the Biometric Processing Privacy Code (the Code) under the Privacy Act 2020 (the Act), on 6th August 2025. The Code will govern the collection and use of biometrics and will specify privacy requirements for agencies and businesses that collect biometric information for the purposes of processing the biometric information.

The Code seeks to provide New Zealanders with confidence about the processing of their biometric information, and their rights and remedies if their information is collected for unlawful purposes.

The Code will be effective on 3rd November 2025, for agencies and businesses that are authorised to or commence with their biometric processing after this date, and 3rd November 2026, for businesses and agencies that are already in the biometric processing business on or before 3rd November 2025.

This white paper was expertly researched and written by **Priya Narasimhalu CIPP(E)**, Content Development Editor for **LexisNexis Regulatory Compliance**. It draws on insights from the *Privacy on Purpose: Navigating the 2025 Amendments in New Zealand and Beyond* webinar, developed in collaboration with Diligent for New Zealand Privacy Week 2025.

We extend our sincere thanks to Priya for her thoughtful analysis and valuable contribution to this important piece.

Decoding the Biometric Processing Code

The Code broadly sets out 13 Rules which apply and replace the existing Informational Privacy principles (IPPs) mentioned under the Act. These are the 13 important rules that are mentioned under Part 2 of the Code.

Rule 1
Purpose of collection

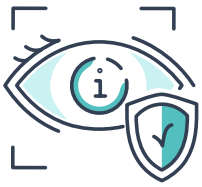
Rule 2
Source of biometric sample

Rule 3
Collection of information from individual (notification)

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 of biometric information

Rule 10
Limits on use of information

Rule 9
Retention of biometric information

Rule 11
Disclosure of biometric information

Rule 12
Disclosure of biometric information outside New Zealand

Rule 13
Unique identifiers

What does the Code apply to?

The Code applies to any organisation, business, and government agencies that collects, use, or process biometric information in automated systems to check, verify, and categorise individuals.

Personal information pertaining to an individual's biometric characteristic as the process of biometric information is referred to as biometric information.

The Code describes what constitutes biometric information and how it can be used. Biometric data is, in essence, the receipt of a biometric sample, for example, a scanned fingerprint, a facial image, or facial recognition data. Once it has been processed and encoded for the purposes of identification or matching, this is considered a 'biometric template'.

> "Biometric data is a scanned fingerprint, a facial image, or facial recognition data.
>
> The Code does not refer to blood, saliva, skin tissue, DNA, brain activity, or nervous system information."

That said, not all biological data falls into this definition. The Code does not refer to blood, saliva, skin tissue, DNA, brain activity, or nervous system information.

The rules are also clear in what circumstances the Code does not apply. For example, if a health agency is processing biometric data as a result of providing healthcare, then the data falls under the Health Information Privacy Code (HIPC), not the Biometric Processing Privacy Code.

The Code will only apply if the health agency works with biometric information that can reasonably not be considered 'health information', or if the biometric information is processed by a non-health service agency, even if the biometric information is health information. Biometric data processed manually, collected through smart consumer devices such as smartwatches or fitness trackers, is also excluded under the Biometric Code.

In short, the Code focuses on situations where biometric information is collected and used outside traditional healthcare contexts or personal devices, highlighting where special care and rules are needed to protect privacy.

Key changes made to the Code

There have been several notable developments in the drafting and consultation process of New Zealand's Biometric Information Privacy Code since the revised version was released for public consultation (December 2024 – March 2025).

October 2021 – Biometric Position Paper

The Office of the Privacy Commissioner (OPC) clarified that biometric information represents personal information under the Privacy Act. The paper recognised the highly sensitive nature of biometric data and described the risks of misuse, surveillance, and "function creep." Organisations implementing biometric technologies were recommended to conduct Privacy Impact Assessments and implement strong security measures.

August 2022 – Public Consultation

The OPC engaged the public, stakeholders, including Māori treaty partners, to discuss regulating biometric data. There were a number of concerns around the use of biometrics, particularly in relation to surveilling citizens and the potential for invasive control over their lives, coinciding with generally accepted citizens' rejection of the use of biometrics without qualified oversight.

December 2022 – Potential consideration of a Biometric Code

The OPC announced plans to explore developing a Code of Practice focused on organisations that collect, store, and manage biometric information.

July–August 2023 – Focused Stakeholder Engagement

The OPC had in-depth discussions with privacy experts, Māori representatives, private sector users, and public sector users. Submissions alerted the OPC to a number of things, including vigilance on risks such as surveillance, profiling, and discrimination, as well as privacy erosion. It is also important to note that the submissions appreciated the advantages of biometric systems - security and convenience.

November 2023 – Explainer Document

The Office of the Privacy Commissioner released a short explainer, and exposure draft, Biometric Code of Practice. The key proposals in the proposed draft included:

- Proportionality Assessment to make sure the biometric process was not excessive or unwarranted.
- Mandatory transparency and notification obligations to keep individuals informed.
- Strict purpose limitations including specific prohibitions on marketing directly from biometrics, use, or inference about an individual's health or emotional state.

The exposure draft also acknowledged the requirement of consultation with Māori where any data was biometrics specific, but also recognised that some categories included (health, genetic, and regular data). The draft was also concerned with building public trust and giving organisations clarity of operation, and coincidentally aligning New Zealand's standards with international best practice. It is intended that the Biometric Code of Practice will host public consultation in early 2024.

April–May 2024 – Public Consultation on Exposure Draft

The consultation focused on three new rules within the draft Code: proportionality requests, mandatory notices, and fair processing limits.

August 2024 – Report on Consultation Feedback

These feedback indicated a public apprehension regarding the increased use of biometric technologies, specifically over surveillance. Organisations sought clearer, useful guidance that would assist with implementing the policy, including applied examples and consistent, plain language drafting. Multiple submissions expressed that the technical language and definitions were unnecessarily complicated and could complicate compliance, indicating that there needs to be clarity in the final Code.

Final updates to the Biometric Processing Code

After the public consultation in December 2024, only minor changes were made to the Code. These changes aim to clarify implementation expectations, while also maintaining the fundamental regulatory aim of the Code. There are some significant changes to note:

- **The Code will officially take effect on November 3, 2025**, with an initial nine-month transition period. Organisations that are already engaged in the collection or processing of biometric information as of the effective date will have a grace period to achieve compliance with the Code, until August 3, 2026. This transitional period is intended to assist in preparations for operational readiness and system change.
- **Rule 1 will continue to require biometric processing to be lawful, necessary, safeguarded, and proportionate.** A significant clarification in the final version of the Code relates to the necessity test: organisations will now have to consider not just if lower risk alternative methods exist, but also how effective they have been in practice. This acknowledges operational realities and will allow for a more granular analysis of the efficacy of biometric system use in situations where methods that do not intrude on privacy are available.
- **Organisations that are conducting trials of biometric systems will be permitted to postpone compliance with the necessity test until the trial is complete**, as long as the trial is proportionate and there are appropriate safeguards in place. All other relevant provisions of the Code will still need to be complied with during the trial period. This flexibility supports the development of information technology systems, while also supporting privacy protections at a minimum baseline.
- The definition of **"biometric categorisation" has been adjusted to remove consumer devices** or services used to only provide people with their own health or personal data (e.g. fitness trackers) or for entertainment and immersive experiences (e.g. virtual try-on filters). This adjustment has been made to ensure that the Code is around high-risk biometric applications and does not capture lower-risk, user-controlled activities.
- The final Code does implicitly restrict the **biometric systems that monitor alertness, fatigue, or attention.** These systems **can only be used for safety-related purposes**, to mitigate risks to life or health. These systems cannot be used for general workplace monitoring, which aligns with the Code's aim to help ensure proportionality and privacy in the workplace.

What Is Biometric Information?

Biometric data includes quantifiable biological or behavioural characteristics that are unique to individuals and can be used for identification or inferred characterisations. Common examples of biometric data include facial features, fingerprints, iris patterns, vocal characteristics, gait, and even behavioural indicators such as typing rhythm.

Unlike other traditional identifiers, biometric data is highly sensitive in nature, due to its uniqueness to the individual, permanence, and ability to reveal more than identity (e.g., health status, emotional state).

Primary functions of Biometric processing

Biometric processing typically exists in three functional types, each with varying implications surrounding privacy and governance.

1

Biometric Verification (One-to-One Matching)

Assessor makes determination if person is who they claim to be based on a comparison against a comparison against a stored reference or biometric data.

2

Biometric Identification (One-to-Many Matching)

Undertakes to determine who a person is based on the comparison between the person's biometric data and a database of individual profiles.

3

Biometric Categorisation

Establishes personal traits or attributes (e.g., age, gender, health, and/or emotions) from biometric data without identity verification.

Core features of the Biometric Processing Code

Under the Code, all 13 rules must be actively implemented and enforced by organisations themselves. These rules are intended to replace the Information Privacy Principles (IPPs) set out in the Act to provide a targeted framework to govern biometric data. Many rules follow the general structure and intention of IPPs (as an example, the meaning of Rules 1, 3, 6, 10, 12, and 13 includes a higher threshold of lawfulness, transparency, individual rights and oversight which is a significant departure). However, Rules 4, 5, 7, 8, 9, and 11 correspond to an IPP, with no significant changes to the meaning of the Rules, to ensure protections remain with the same core privacy protections but tailored to the risks of biometric technologies.

Rule 1
Purpose of Collection

Organisations shall only collect biometric information for a lawful, specific, and necessary purpose, where there is no effective and safe alternative with lower risk. Organisations must have strong privacy protections in place, assess whether benefits of collecting biometric information outweighs risks, and assess whether there are cultural impacts, particularly for Māori.

Rule 2
Source of Biometric Information

Organisations must collect biometric samples directly in relation to the individual, unless doing so contravenes an exemption, i.e. the individual consented to third-party collection, or the collection prevents a serious threat to life or health.

Rule 3
Collection of information from individual

Organisations must be transparent regarding the collection as well as the purpose of collection, available alternatives, and individual rights, which must all be clear and accessible to individuals.

Rule 4
Manner of collection of biometric information

Organisations must collect biometric information in a manner that is lawful, fair, and without unreasonable intrusion. When collecting information from children and young people, organisations need to take extra care.

Rule 5
Storage and Security of Biometric Information

Organisations must put in place layered technical, organisational, and physical safeguards that protect biometric information from loss, unauthorised access, or appropriation, and must have processes in place for all breaches or security incidents that occur to biometric information.

Rule 6
Access to Biometric Information

Individuals will be entitled to know whether an organisation holds their biometric information, what type it is, and have access to it, unless a legal exemption applies.

Rule 7
Correction of Biometric Information

Individuals will be able to request for corrections to their biometric information, or request that a statement of correction be added if the organisation disagrees, with reasonable steps taken to notify anyone else who received the data.

Rule 8
Accuracy of Biometric Information

Organisations must take reasonable steps to confirm that biometric information is accurate, complete, up to date and relevant before using or disclosing it and should factor in the reliability and accuracy of the biometric systems being used.

Rule 9
Retention of Biometric Information

Organisations must irrevocably and securely dispose of the biometric information once it is no longer necessary for its lawful purpose, and organisations must have a clear oversight role with third-party providers in managing the ongoing storage, retention, and disposal of biometric information.

Rule 10
Limits on Use of Biometric Information

Organisations shall only use biometric information for the stated purpose for which it was collected and must not use this information for findings as sensitive biometric identity classifications (i.e., health-related information.), unless a clear exception applies.

Rule 11
Disclosure of Biometric Information

Biometric information will not be disclosed unless there is a legitimate basis such as consent, lawful authority, stated purpose or there is a risk of serious harm, with reasonable basis for the decision.

Rule 12
Disclosure of biometric information outside New Zealand

Biometric information will only be transferred overseas if the recipient is sufficiently protective, bound by the Code or equivalent privacy laws, or the individual authorises the transfer.

Rule 13
Unique Identifiers

Organisations shall only assign or use unique identifiers, including biometric templates, in accordance with constraints against unnecessary or inappropriate identification.

Bridging the Gap: Navigating New Zealand Privacy Compliance in a Digital Age

As digital technologies affect how personal information is collected, processed, and otherwise shared, New Zealand's privacy landscape is entering a formative phase of adaptation and development. The emergence of biometric systems, AI-based analytics, and increasingly complex cross-border data flows has revealed the limitations of conventional compliance systems, underlining the need for a more adaptive, risk-responsive type of governance.

> Organisations are required to take responsibility for proactive, principled governance."

Biometric systems are increasingly embedded in the delivery of services and infrastructure for identity verification and surveillance. The utilisation of biometric systems also introduces significant privacy risks and cultural sensitivities; organisations are required to move beyond minimum compliance and take responsibility for proactive, principled governance. To this end, two basic practices, namely Privacy Impact Assessments (PIA) and consultation with affected communities are recommended. These simple tools help to remind practitioners to operationalise the principles of necessity, proportionality and transparency, as noted in the Biometric Processing Privacy Code, to ensure that processing of biometrics is lawful and secure, but also ethical and socially legitimate.

Privacy Impact Assessments: A Strategic Compliance Tool

Privacy Impact Assessments (PIAs) are a vital tool to identify and reduce privacy risks before engaging in biometric processing - they allow organisations to determine whether proposed Activities meet the requirements of the Code, including lawful collection of data (Rule 1), transparency (Rule 3), fairness (Rule 4), and data minimisation (Rule 9). A comprehensive and well-documented PIA should do the following:

- Identify stages in the biometric data lifecycle, including collection, storage, use, disclosure, and disposal, before assessing the privacy risks associated with those stages.
- Consider legal risks and ethical risks, which include determining any risks of harm to individuals, especially for vulnerable individuals.
- Assess organisational design decisions, including the choice of biometric modality, matching algorithms, and data retention limits.
- Document privacy safeguards, such as encryption, access controls, and notification procedures for management of a data breach.
- Support accountability for considering and addressing privacy risks prior to implementation.

> Failure to conduct a meaningful PIA may violate several rules under the Code, especially in relation to high-risk processing or activities for which the processing is novel."

Organisations do not need to use a prescribed template for a PIA. The Office of the Privacy Commissioner offers guidance on comprehensive PIAs to support a rigorous PIA process. Notably, failure to conduct a meaningful PIA may violate several rules under the Code, especially in relation to high-risk processing or activities for which the processing is novel.

Consultation: Building Trust and Cultural Legitimacy

Consultation is more than just a good practice; it can also turn out to be a requirement of employment law, human rights law or treaty obligations. By engaging those affected and their communities, we can garner insight into the social legitimacy of, and cultural safety and responsiveness of biometric processing in relation to stakeholder concerns.

Good consultation has the following qualities:

- **Inclusive:** Think about whose biometrics will be affected. If possible, consult people directly and consider consulting broader representative groups, e.g. unions, advocacy groups or cultural organisations.
- **Expert informed:** When undertaking consultation, see if you can engage with those who have technical, legal or cultural experience with the biometric system. This might be privacy practitioners or ethicists or Māori advisors or disability advocates.
- **Transparent and timely:** Be clear about the rationale, scope, and impact of the proposed processing. Allow sufficient time for response and genuinely be prepared to change the proposal based on the response.
- **Culturally responsive:** If the biometric data is Māori data or there is Māori interest, consider requiring consultation with iwi, hapū and/or Māori governance entities consistent with Te Tiriti o Waitangi and to ensure tikanga-based stewardship of the data.

Consultation should not be treated as a one-off exercise. Instead, it should be embedded into the design, implementation, and review phases of biometric systems, ensuring that individuals retain agency over how their identity is captured and used.

Bridging Legacy Systems and Emerging Risks

Though biometric technologies can provide significant benefits to individuals, agencies, and society including increased security, easier identity verification, and improved delivery of services they also introduce a complicated set of privacy risks and ethical issues. These risks extend beyond the failure of a system to function; they also exist through intentional operation of biometric systems. Notably, the level of risk and the degree to which biometric processing is intrusive are determined by the modality type, the context in which the modality is being used, and the identities of the populations involved. Factors such as the amount of personal information involved, the level of deployment, the risk of harm to the population, and the consequences of decision-making based on biometrics, all factor into the risk determination.

Biometric data is remarkably sensitive because its origin is the human body and it is deeply intertwined with personal identity and dignity. Unlike a password or similar identifiers, biometric characteristics, such as fingerprints, facial features, or patterns of the iris, are relatively permanent. If biometric data is compromised, it cannot be easily replaced, increasing the risk of irreparable harm. The uniqueness of biometric characteristics makes them an effective means of identification and authentication but also increases the risk of harmful outcomes associated with inappropriate use. In addition to technical sensitivities, biometric information may also embody cultural values. For example, for Māori, biometric data is relating to whakapapa or genealogy, making an association for a person to an ancestor and ties to whānau, hapū, and iwi. In the case of facial recognition, biometric data may include recording of traditional

“The uniqueness of biometric characteristics makes them an effective means of identification and authentication but also increases the risk of harmful outcomes associated with inappropriate use.”

> Secondary data can provide indications of a person's health status, emotional state, or behavioural characteristics."

markings, such as tā moko or moko kauae, that are imbued with cultural meaning and sacred. Processing these data points, without requisite protections or consultation, may not only breach privacy rights but also harm cultural integrity and erode trust.

Biometric systems can provide secondary data that even goes beyond what biometric systems are intended to obtain. Secondary data can provide indications of a person's health status, emotional state, or behavioural characteristics. It can be collected even when individuals are not aware or consenting to the collection, and there are risks of unintended profiling and function creep. In addition, biometric technologies stand to enable mass surveillance or deployment of profiling, especially when put to scale in public-facing technologies or systems designed for surveillance purposes. For example, using live video from CCTV in order to do facial recognition is a loaded example of algorithmic technologies deployed for uncontrolled profiling of an individual. The risks of data collection, secondarily to biometric identification, become magnified when data is collected without knowledge of individuals, integrated with other datasets, and then potentially used for automated decision systems with little to no human involvement. In these cases, an individual may be monitored, profiled, classified, or excluded without any knowledge or recourse, and it may have an even greater impact for marginalised or vulnerable groups.

Another area of concern regarding biometric governance is function creep. Function creep is when biometric data is collected for one purpose, but then is used for a different, often non-related, purpose. For example, a government agency may collect biometric information to enable secure access to online services but later repurpose that data for law enforcement or immigration control. Such secondary uses may not have been anticipated by the individuals concerned, and appropriate safeguards may not be in place. Function creep undermines the principle of purpose limitation and increases the risk of surveillance, misuse, and erosion of public trust.

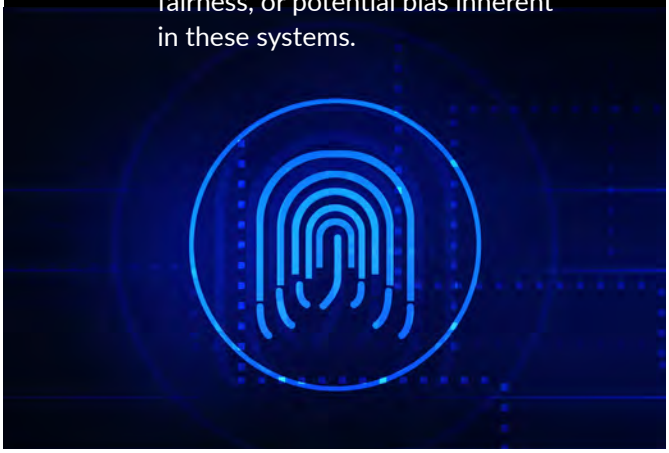
Biometric Governance Concerns

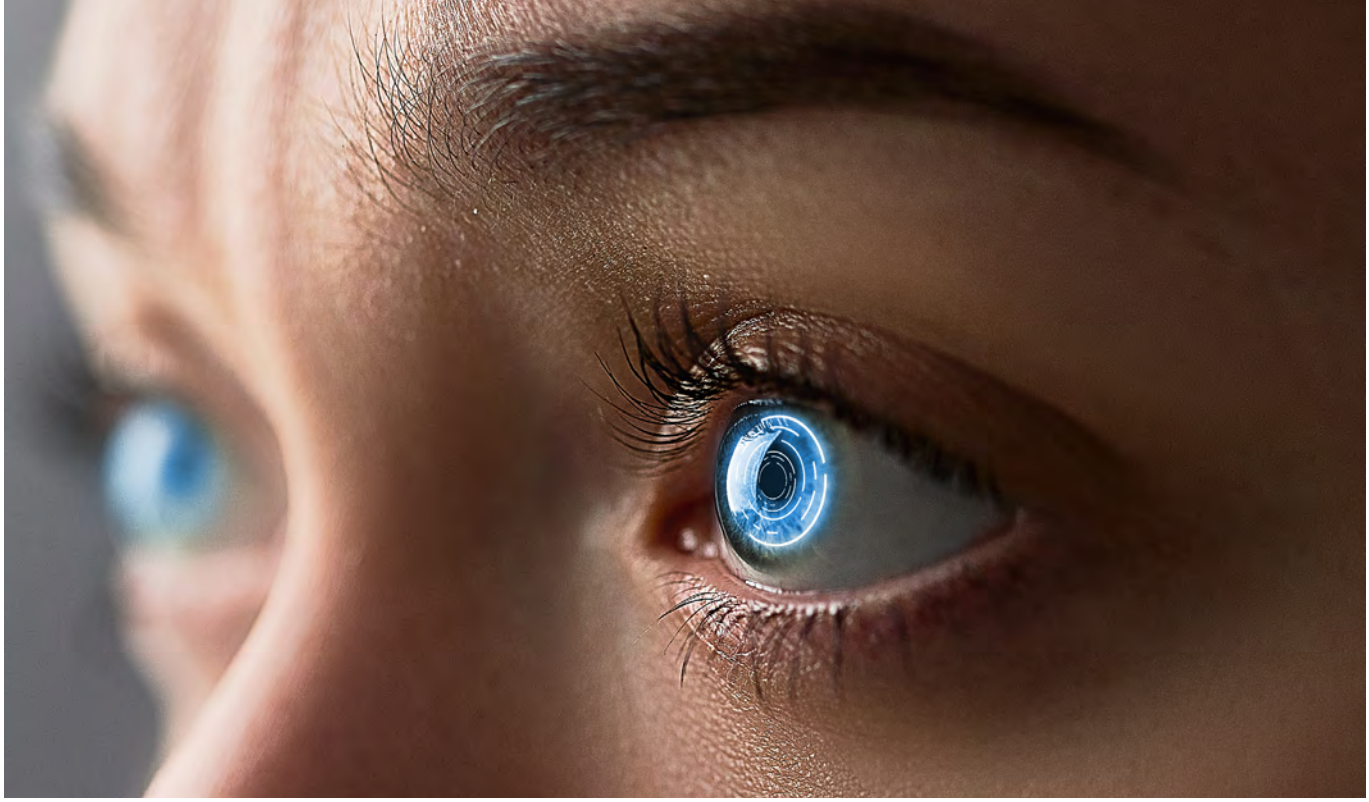
1. Function Creep
Biometric data collected for one purpose may later be repurposed for unrelated uses (e.g., from securing online services to law enforcement), which undermines the principle of purpose limitation and increases the risks of surveillance and misuse without proper consent or safeguards.

2. Biometric Data Cannot Be Easily Replaced
As biometric characteristics (e.g., fingerprints, facial features, iris patterns) are permanently tied to an individual's body, any compromise of this data can lead to irreparable harm. Unlike passwords or tokens, biometric data cannot be easily changed if it falls into the wrong hands.

3. Lack of Transparency and Control
Biometric systems may operate in ways that are not perceptible to individuals:

- They can collect secondary data beyond what is necessary, such as indicators of health or emotional state.
- Collection may occur without the individual's informed consent, especially when used in public surveillance (e.g., live facial recognition via CCTV).
- Proprietary algorithms and commercial secrecy make it difficult to assess the accuracy, fairness, or potential bias inherent in these systems.





These risks become further entrenched when there is a lack of transparency and control. Biometric systems may operate in ways that cannot be perceived, collecting information when individuals were unaware and could not opt out of the collecting process. For example, facial recognition technology may be employed to identify individuals without notice in the scene or from a distance, taking away the opportunity for informed consent. In some cases, individuals are required to submit biometric data as a condition of receiving a critical service, which effectively removes any meaningful choice in the process. Additionally, the algorithms driving biometric systems are frequently proprietary and protected by commercial secrecy. Without transparency, it is often impossible to know what processes were followed to make a decision, evaluate what limits the process holds regarding accuracy of results or to mount a challenge when presented with an error when biometric processing provides rights punishment, or eligibility.

> “Accuracy, bias, and discrimination remain endemic issues related to biometric technologies. False matches and false non-matches can have life-altering impacts for individuals. The consequences can be significant, such as wrongful investigation, incorrect non-verification of a person’s presence, disallowing access, or exclusion from a service.”

Accuracy, bias, and discrimination remain endemic issues related to biometric technologies. False matches and false non-matches can have life-altering impacts for individuals. The consequences can be significant, such as wrongful investigation, incorrect non-verification of a person’s presence, disallowing access, or exclusion from a service. The incidence of errors is not uniformly distributed. Biometric systems may not perform as effectively for certain groups, including women, minority ethnic groups, or disabled persons. Additionally, there are occasions where bias may enter the biometric algorithm data set when prior databases have allowed over-representation of one or more populations. This can reinforce systemic inequalities and result in discriminatory outcomes, especially when biometric data is used in high-stakes decision-making contexts.

In conclusion, these risks emphasise the need for strong, culturally safe, ethical governance frameworks. The Biometric Processing Privacy Code provides a formalised approach for managing the risks above, but its utility will depend on the degree to which organisations can understand and address the unique complexities that arise with biometric processing. Active strategies such as Privacy Impact Assessments, real engagement with affected communities, and designing systems with transparency will be significant to assist accountability in the practical implementation of biometric technologies in ways that respect individual rights, honour cultural values, and maintain public trust.

Addressing the Gaps: Proactive Compliance and Transparency

As biometric technologies penetrate deeper into identity systems, government, and enterprise, regulations in New Zealand also keep pace with their typical challenges. Since biometric information is extremely personal, culturally priceless, and often non-replaceable, exceptional privacy protection becomes necessary. Nevertheless, most organisations continue to have gaps in operational preparedness in areas of openness, communication to and from stakeholders, and control over cross-boundary information flows.

Overcoming these challenges requires an adjustment in strategy from reactive compliance to proactive governance. Organisations would have to construct systems not only to today's legal demands, but to systems amenable to future advances in regulations. This would include maintaining extensive data acquisition registers maintaining separate and distinct information on direct and indirect means of acquisition, maintaining robust systems of notification, and being active players in involving affected communities in specific instances in particular where cultural protocols such as whakapapa come into play.

Transparency is woven throughout this plan. When citizens understand how their biometrics are being collected, utilised, and protected, trust follows, and compliance becomes strong. Periodic privacy audits, communication to stakeholders, and risk assessments become strong tools to ensure biometric systems not only operate technically but remain socially legitimate.

Comparative Challenges in Cross-Border Transfers: New Zealand's Biometric Processing Privacy Code vs the GDPR

Rule 12 of the Code sets New Zealand's framework for cross-border biometric data disclosures. It aims to ensure the biometric data disclosed offshore has similar protections to New Zealand's code protections, emphasising privacy and cultural sensitivity with respect to Māori data.

> Rule 12 of the Code sets New Zealand's framework for cross-border biometric data disclosures."

However, the conformance challenges are stark. Unlike the EU's General Data Protection Regulation (GDPR) that has lists of adequacy and standard mechanisms like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) approved by each EU member nation, New Zealand has no "prescribed countries" or pre-approved contractual templates for transferring biometric data, requiring an organisation to determine whether each legal regime provides adequate protection on a case-by-case basis. This creates a complex

and sometimes unclear process for organisations seeking to transfer data outside of New Zealand, potentially regularly or at high volumes. The requirement to provide "comparable protection" is subjective as well.

"The Code requires attention to cultural impacts, restricts specific forms of biometric classification, and imposes a requirement to show proportionality in processing."

Organisations must consider breach notice processes, individual rights to access and correction, limits on biometric categorising, and the sensitivity of the biometric information. These considerations are discretionary in nature and are likely to vary across organisations creating additional compliance risk and the need to develop bespoke safeguards.

The Code biometric-specialised commitments increase operational complexity. In addition to standard data protection, the Code requires attention to cultural impacts, restricts specific forms of biometric classification, and imposes a requirement to show proportionality in processing. Although these policies strengthen individual protection, they also require specialised expertise and intensive compliance commitments.

Enforcement also differs markedly. Breaches of New Zealand law shall incur fines of up to $10,000, which is limited compared to the GDPR's potential penalties of up to EUR 20 million, or 4% of an annual global revenue, binding corrective measures and harmonised enforcement by EU member states.

In practice, Rule 12 involves a reliance on organisational judgement, detailed contracts, and informed consent. Transfers are only permitted if there is reasonable confidence that the protections to be provided by the overseas recipient will be comparable to the Code, or an exception expressly applies. Organisations are required to document adequately their decision-making, interpretation of the overseas legal framework applicable, and development of specific, tailored safeguards without standardised tools or clarity in regulatory direction.

"Organisations are required to document adequately their decision making, interpretation of the overseas legal framework applicable, and development of specific, tailored safeguards without standardised tools or clarity in regulatory direction."

In summary, Rule 12 promotes New Zealand's commitment to strong, culturally aware protections of biometric information, but also entails greater subjectivity, administrative complexity, and legal uncertainty than GDPR's robust and structured approach. Operating entities must engage with these complexities with caution to remain compliant and engage in safe and culturally appropriate practices more broadly.

Proactive Transparency in Biometric Processing: A Cornerstone of Trust aand Compliance

In biometric governance, transparency becomes not only a regulation-driven requirement but also a strategic necessity. The institutions which take it upon themselves to educate people inside and out on the gathering and processing of biometric information earn trust, minimise resistance, and prove to be accountable. Providing people with transparent information regarding why biometric information is being gathered, who would process it, and who would have access to it ensures legal compliance and ethical interaction.

> “Individuals should be made aware of their access, correction, or complaint rights regarding their biometric information.
>
> Active transparency also helps reduce operational and legal risks.”

Effective transparency also means providing specific, context-appropriate notification to people. People must be advised that biometric information is being gathered, and they must be specific regarding the kind of information being gathered, for instance, “a fingerprint scan” and not a generic phrase such as “biometric sample.” The intent of gathering must also be clearly expressed in specific, understandable language, for instance, “to identify people on a watchlist gaining access to our facility,” and not in generalised terms such as “security purposes.” This helps people decide and comprehend the ramifications of being involved.

Entities must provide any available substitutes for biometric processing, access procedures for those substitutes, and recipients of biometric information. This means providing data custodian contact information, outlining legal authority for data collection, and explaining the consequences of opting out. Individuals should be made aware of their access, correction, or complaint rights regarding their biometric information. Furthermore, as appropriate, entities must disclose retention periods, complaint mechanisms, and sources of proportionality reviews or trial documents.

> The Code is built on privacy by design and default, mandating safeguards such as encryption, deletion protocols, and breach notification, as well as strict rules for cross-border transfers."

Under the minimum notification requirement, certain details must be made known in advance of or at the time of data collection. This includes recognition of an acknowledgment that biometric information is being collected, why it is being collected, and any available options. It is recommended that organisations provide this information in easily readable formats, including through clear language, prominent signage, and adequate oral or written communication. Additionally, accompanying information must be made known as soon as practicable after collection, thus ensuring people remain informed throughout the whole data life cycle.

Active transparency also helps reduce operational and legal risks. Clear and early communication minimises confusion, avoids grievances, and strengthens organisational credibility. Notification processes must be tailorable to specific contexts: voluminous disclosure is necessary at time of enrolment, whereas continuing procedures may necessitate regular reminders. In any event, any variation in type of biometric information taken, or in how it could be used, ought to initiate new notifications.

Although there are some exceptions to notification, including occasions upon which disclosure would prejudice law enforcement or research integrity entities, transparency ought to be the default position as often as possible. Open, expedient, and complete communication regarding biometric processing is conducive to ethical data stewardship, fortifies public trust, and complies with shifting expectations regarding privacy. The Code is built on privacy by design and default, mandating safeguards such as encryption, deletion protocols, and breach notification, as well as strict rules for cross-border transfers. Strong leadership and governance are vital—boards and executives must prioritise privacy, allocate resources, and foster accountability through training, audits, and risk reviews. Technology tools can help by automating compliance, monitoring risks, and streamlining responses. Ultimately, privacy is not just a legal duty but also a competitive advantage, and the Code provides a modern, ethical, and culturally aware framework for trustworthy biometric governance.

Step-by-Step Design: Voice Biometrics in Banking

This example illustrates how proactive transparency can be operationalised in a way that is both compliant and user-friendly, reinforcing trust while maintaining regulatory integrity.

1. A bank uses voice biometrics to verify customers during phone interactions.

2. Recording sent to customer at the point of enrolment, customers receive a recorded message that outlines all relevant information, including the nature and purpose of the biometric collection, available alternatives, and where further details can be found (e.g. the bank's website).

3. Customers are given the choice to opt into the voice verification system or select a less secure alternative.

4. On subsequent calls, when customers choose to verify their identity using voice biometrics, they receive a brief reminder about the collection and are directed to where more information is available.

5. This satisfies the minimum notification requirement. Because full disclosure was provided at enrolment, the bank is not required to repeat all details during each interaction, even if the caller is not enrolled or is later identified as a fraudster.

Conclusion

As biometric technologies become further integrated in organisational systems across New Zealand, a proactive and well-structured approach to privacy compliance is no longer optional; it is imperative. Meeting the requirements of the Biometric Processing Privacy Code 2025 demands further than procedural alignment; it calls for integrated governance, robust data management, and a provable culture of transparency and accountability. Organisations must be prepared to undertake comprehensive privacy impact assessments, conduct nuanced proportionality evaluations, and, where necessary, seek foreign expertise to ensure their practices meet both the letter and spirit of the Code.

For entities already engaged in biometric processing, mature planning is essential. This includes reviewing the applicability of the Code to current operations and initiating careful assessments to evidence compliance, peculiarly with foundational obligations such as those under Rule 1. For organisations considering the deployment of biometric systems, controlled trials offer an invaluable opportunity to evaluate functional feasibility, assess privacy risks, and refine proportionality justifications before round implementation.

> By aligning domestic practices with the Biometric Processing Privacy Code 2025 and harmonising them with global standards, organisations can build open trust, reinforce reputational strength, and ensure that biometric data is managed lawfully, transparently, and with ethnic sensitivity at its core."

Ultimately, a live privacy programme is not defined only by regulatory adherence. It reflects an organisation's commitment to moral data stewardship, respect for individual rights, and readiness to operate responsibly in a digitally complex and culturally different environment. Embedding privacy into organisational culture through leadership accountability, staff training, stakeholder engagement, and continuous review positions organisations to navigate evolving expectations with confidence and integrity. By aligning domestic practices with the Biometric Processing Privacy Code 2025 and harmonising them with global standards, organisations can build open trust, reinforce reputational strength, and ensure that biometric data is managed lawfully, transparently, and with ethnic sensitivity at its core.

In a fast-moving digital world, privacy demands active engagement. As biometric data becomes part of ordinary processing, awareness, not avoidance, is key. Aware of our rights and insisting on transparency turns peaceful subjects into empowered participants.

Your Free Demonstration

Request a free demonstration of the LexisNexis® Regulatory Compliance **Privacy and Data** Security compliance register →

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance helps you forge a clear path to compliance.

With LexisNexis content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.

- Find relevant obligations faster with jargon-free registers that are aligned with your business processes.
- Stay up to date with near real-time alerts delivered straight to your inbox when you may be impacted by regulatory change.
- Explore your compliance obligations under a particular regulator, or a particular compliance source, with SourceData.
- Engage with the wider compliance community and LexisNexis experts through the Community Portal, our self-support platform.
- Access comprehensive, current LexisNexis content that meets your unique needs, with eight core modules relevant to all businesses, and over 90 industry-specific modules.

Authored by leading legal, attorney and industry experts, and supported by flexible technology that works the way you do, LexisNexis Regulatory Compliance gives you peace of mind while saving time and money.

Call 0800 800 986

Email compliance@lexisnexis.co.nz

Visit www.lexisnexis.co.nz/compliance

About Diligent

Diligent is the leader in governance, risk and compliance. One million users and more than 700,000 board members and leaders rely on Diligent software to connect insights across governance, risk, compliance, audit, and ESG to drive greater impact and lead with purpose.

Visit www.diligent.com

LexisNexis® | *Regulatory Compliance*