

Biometric Processing Privacy Code 2025

The Biometric Processing Privacy Code 2025, issued under the Privacy Act 2020, regulates how organisations collect, hold, and use biometric information for the purposes of biometric processing.

We collect biometric information (e.g., facial recognition) for the purpose of verifying customer identity under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (“AML/CFT Act”) obligations. This processing is lawful under the Privacy Act 2020 and the AML/CFT Act.

1. Why are we collecting your biometric information?

Under the Anti-Money Laundering and Countering Financing of Terrorism Act, we are required to collect and verify the identity of our clients.

2. How are we collecting your information?

We contract RealAML to undertake biometric processing for us. The RealAML Biometric Privacy Compliance Statement is available here: [NZ Biometric Privacy Compliance Statement](#).

3. Who will receive your information?

Tompkins Wake will receive your biometric information to use for our business purposes.

4. What if I don't agree to the collection of biometric information?

Biometric information may only be collected if the biometric processing is necessary for the purpose. An alternative means of collection is non-biometric processing, for example a manual verification process whereby your proof of identify and proof of address are certified by a trusted referee.

5. We can only collect biometric information proportionate to the likely impacts on people.

We have assessed the scope, extent and degree of privacy risk from the biometric processing, and whether the benefit of achieving the lawful purpose through the biometric processing outweighs the privacy risk. We have also considered potential cultural impacts, particularly Māori perspectives, to ensure respectful and culturally safe practices in the collection and storage of biometric information.

6. How is your biometric information used?

We only use your biometric information for verifying identification to meet our legal obligations.

Your biometric information is not used to detect emotions, health status or demographic traits.

We will not disclose your biometric information to another person or organisation unless there are valid grounds for disclosure.

6. How is my biometric information stored?

Your biometric information is encrypted and stored securely. Access is restricted to authorised staff members only. Under the AML/CFT Act data retention is limited to at least five years after the completion of the transaction or at the end of the business relationship with the customer, followed by secure disposal.

7. What are my rights in relation to my biometric information?

You can request access to your biometric information, which we may decide to provide to you unless we withhold some or all under the law. You also have the right to ask us to correct your information if you think it is inaccurate. Correcting your information could involve removing that information from our system and reconducting the biometric process to gather a new image. Alternatively, if we do not agree that the information needs correcting, you can ask us to attach a “statement of corrections” to your records.



You can contact us at aml@tompkinswake.co.nz in respect of your biometric information.

If you have concerns about your biometric information you can make a complaint to the Tompkins Wake Privacy Officer at privacy@tompkinswake.co.nz or the [Privacy Commissioner](#).