



# Biometric Privacy Code 2025: NZ Compliance Guide

*Last updated - Oct 01, 2025 at 4:00PM*

Web:	<a href="https://timedock.com">https://timedock.com</a>
Email:	<a href="mailto:info@timedock.com">info@timedock.com</a>
International:	(+64) 9 444 1384
Local phone:	(09) 444 1384

# Table of Contents

What is the Biometric Processing Privacy Code 2025? .....	3
Key Dates and Deadlines.....	3
Compliance Requirements.....	4
Why Biometric Time Clocks Will Struggle .....	4
Biometric Alternatives .....	4
Next Steps for Employers.....	4
Summary .....	5
Further Reading .....	5

The *Biometric Processing Privacy Code 2025* is a major update to New Zealand privacy law. It introduces strict rules for biometric systems such as fingerprint and facial recognition. This guide explains what the Code is, when it comes into force, what businesses must do to comply, and the alternatives to biometric time tracking.

## What is the Biometric Processing Privacy Code 2025?

The Biometric Processing Privacy Code 2025 is a legal framework introduced by the Office of the Privacy Commissioner to regulate how biometric data is collected, stored, and used in New Zealand. It applies to technologies such as:

- Facial recognition scanners.
- Fingerprint readers.
- Iris/retina scans.
- Voice ID and similar biometric identifiers.

The purpose of the Code is to limit unnecessary biometric use in everyday workplace settings and require stronger justification, transparency, and security wherever biometrics are used.

## Key Dates and Deadlines

<b>3 November 2025</b>	Any <i>new biometric system</i> must comply immediately.
<b>3 August 2026</b>	All <i>existing biometric systems</i> must be updated.
<b>Trial Option</b>	Organisations may test biometric systems for up to six months (with one possible six-month extension), but these trials do not delay the compliance deadlines.

## Compliance Requirements

- Conduct a *necessity and proportionality assessment* to prove biometrics are essential.
- Provide a *non-biometric alternative* such as RFID, PIN, or mobile clock-ins.
- Update *privacy notices and consent processes*.
- Strengthen *security controls, retention policies, and vendor contracts*.

## Why Biometric Time Clocks Will Struggle

- Most workplaces cannot prove biometrics are strictly necessary.
- Alternatives like mobile apps and RFID cards achieve the same results.
- Vendors may be forced to run *dual systems* → higher costs, complex onboarding.
- Only very high-security environments can justify biometric-only solutions.

## Biometric Alternatives

Non-biometric time tracking systems provide:

- Simpler compliance.
- Lower operating costs.
- Higher employee trust.

## Next Steps for Employers

1. Audit your time tracking systems.
2. If using biometrics, complete a necessity assessment.
3. Provide a non-biometric option by law.
4. Review vendor contracts and data security.
5. Consider switching to a *non-biometric provider like TimeDock*.

## Summary

The Code is a turning point. Biometric systems will struggle to justify themselves under New Zealand law. Most employers will either pay more to maintain dual systems or switch to a *compliant, privacy-friendly alternative like TimeDock*.

## Further Reading

For more detail on the Biometric Processing Privacy Code 2025, see:

- [Office of the Privacy Commissioner – Media Release](#)
- [MinterEllisonRuddWatts – Biometric Processing Privacy Code Now in Force](#)
- [Simpson Grierson – New Privacy Rules for Biometrics in New Zealand](#)