v.25.11.6

Biometric Time Tracking

Privacy Impact Assessment and Compliance Kit

In force
November 2025

Biometric Privacy

What to know, and how to go about it...

In force
November 2025

Will it affect my business?

Biometric Processing is now its own privacy code, under New Zealand law.

The purpose of this compliance kit is to help New Zealand organisations decide if biometric time-clocking (and other use cases) is appropriate under the Biometric Processing Privacy Code 2025, and implement it lawfully, safely and fairly.

The Code expects biometrics to be lawful, necessary, effective and proportionate, and not used if a less intrusive method would achieve the same result (e.g., key fob, swipe card, PIN, or mobile clock-ins).

Quick check:

Use the Biometric Qualification flowchart (see next page) to scratch-test your business:

1. Is it tied to a lawful business purpose?
2. Is biometric collection actually necessary to achieve that purpose?
3. Do the benefits outweigh the privacy and cultural impacts?
4. Have you completed a Privacy Impact Assessment (PIA)?

Proceed only if all answers are "Yes" and you offer a non-biometric option alongside your fingerprint, face-recognition or other biometric time docking.

If **any answer** on the following page is "**No**", use a non-biometric method.

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

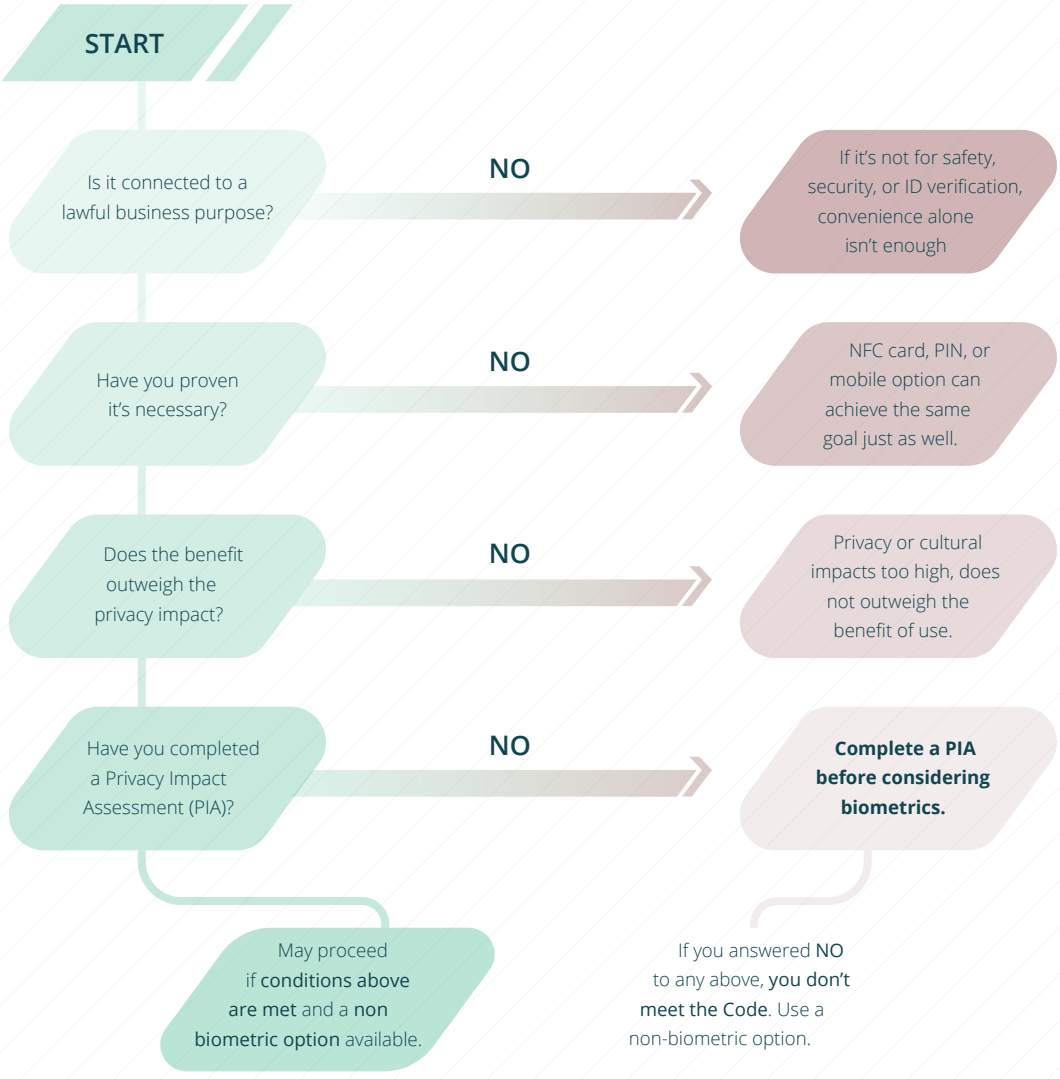
Website
https://timedock.com

New Zealand Made

Tentatively,
where do you sit?

Biometric scratch test

Check if your organisation can lawfully use biometrics, under the New Zealand Biometric Processing Privacy Code 2025.



P.I.A. ON PAGE 10

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

At a glance

The Biometric Processing Privacy Code 2025

Guidelines for New Zealand Organisations Using Biometric Time-Tracking

Updated September 2025

1. Purpose of Guidelines

1.1 Timedock Limited (Timedock) provides these Guidelines to offer high-level guidance to New Zealand organisations assessing the potential use of **biometric time-tracking technologies** (for example, fingerprint scanners, facial recognition, iris or retina scanning, and voice identification) as part of employee time recording.

These Guidelines are current as at **30 September 2025**.

1.2 Biometric technologies may only be used in appropriate circumstances. Under the **Biometric Processing Privacy Code 2025**, organisations must demonstrate that using biometrics is lawful, necessary, effective and proportionate to their intended purpose, and that no less intrusive method (such as a card, PIN or mobile clock-in) would achieve the same result. Each organisation's circumstances should be evaluated individually.

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

1.3 These **Guidelines are not legal advice** and are not intended to provide specific or comprehensive guidance. Organisations should make their own assessments about whether biometric time-tracking is appropriate for their organisation before implementing any such system.

2. Privacy Considerations

2.1 Biometric time-tracking systems collect **biometric information** about individuals. This may include unique identifiers such as fingerprint templates, facial feature vectors, iris patterns, voice prints or other physiological or behavioural characteristics. Under the **Privacy Act 2020** and the **Biometric Processing Privacy Code 2025**, biometric information is sensitive personal information.

2.2 The Code replaces certain Information Privacy Principles (IPPs) for biometric processing and imposes additional obligations. Organisations must ensure that any biometric collection has a **lawful purpose**, is **necessary** for that purpose, and is **proportionate** to the intrusion on privacy. The Code also requires that individuals are told what data is being collected, why, how it will be used, how long it will be kept, and what alternatives exist.

2.3 Privacy obligations should be evaluated on a case-by-case basis. Every organisation has different factors to consider in determining **what** and **how** biometric information can be collected and used.

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

2.4 Before deciding whether to use biometric time-tracking, organisations should conduct a **necessity and proportionality assessment** and consider preparing a **Privacy Impact Assessment (PIA)**. A PIA helps assess and address privacy risks and should examine whether less intrusive alternatives can achieve the same purpose.

2.5 From a privacy perspective, organisations should conduct thorough analysis before implementing any biometric system. This includes reviewing legal obligations, assessing necessity, ensuring appropriate safeguards, and planning for data retention and deletion. If biometrics are not strictly necessary, the Code requires a **non-biometric alternative** (such as cards, PINs or mobile clock-ins) to be offered.

2.6 What not to do:

- Do not implement biometric time-tracking without first completing a necessity assessment and considering privacy obligations.
- Do not ignore current privacy guidance or the requirements of the Biometric Processing Privacy Code 2025.

2.7 What to do:

- Carefully analyse the Biometric Processing Privacy Code 2025 and the Privacy Act 2020 before deciding to implement biometrics.
- Conduct a necessity and proportionality assessment and consider preparing an organisation-specific PIA.
- Ensure employees are informed about what biometric data will be collected, why it is required, how it will be used and how long it will be stored, and advise them of any non-biometric alternatives.
- Implement strong data security measures and retention policies for biometric information.
- Keep up to date with current guidance from the Office of the Privacy Commissioner.

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

3. Employment Considerations

3.1 Employers must consider employment obligations (in addition to privacy obligations) when looking to introduce biometric time-tracking. Changes to workplace practices may require consultation with employees and, in some cases, their consent.

3.2 When introducing biometrics, organisations should act in good faith and consider whether employees have valid concerns or cultural objections. A less intrusive alternative must be provided where biometrics are not essential.

3.3 Organisations should review employment agreements and policies to ensure they allow for changes to time-recording practices. Consult your employment agreements or collective agreements to determine whether employee consent is required.

3.4 Timedock recommends that organisations obtain legal advice on employment law requirements if unsure about how to introduce biometric time-tracking or alternative methods.

3.5 What not to do

- Do not implement biometrics without considering employment obligations and consulting employees.

3.6 What to do

- Act in good faith when proposing biometric time-tracking.
- Review employment agreements and obtain legal advice if needed.
- Consult with employees and consider their feedback before implementing biometrics.

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

4. Consider Alternatives

4.1 Taking into account the privacy and employment considerations discussed above, organisations should consider whether **alternative avenues for time recording** are available and whether the same objectives can be achieved without collecting biometric data.

4.2 Non-biometric options include key fobs, NFC cards, barcode IDs, PIN codes or mobile app clock-ins. These methods reduce privacy risks and are generally easier to implement and maintain. Under the Code, organisations must offer such alternatives if biometrics are not strictly necessary.

4.3 What to do

- Evaluate whether non-biometric time-tracking methods are suitable for your organisation.
- Weigh the privacy, security and cost implications of different time-recording options.

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

5. Summary and Disclaimer

5.1 The use of biometric time-tracking is dependent on the specific circumstances of each organisation and should be analysed on a case-by-case basis. Under the Biometric Processing Privacy Code 2025, organisations must demonstrate that biometrics are necessary and proportionate, and must offer alternatives where appropriate.

5.2 These Guidelines are for general information only and do not constitute legal advice. Timedock does not provide any representation or assurance that biometric time-tracking may be lawfully implemented in all circumstances. Organisations should obtain legal advice about the use of biometric technologies in their specific circumstances.

Further Reading

For additional information on the legal requirements and privacy principles discussed in these Guidelines, see:

- **Office of the Privacy Commissioner**
  Biometric Processing Privacy Code 2025.
  https://www.privacy.org.nz/privacy-principles/codes-of-practice/biometric-processing-privacy-code/

- **MinterEllisonRuddWatts** – Biometric Processing Privacy Code now in force: what organisations need to know.
  https://www.minterellison.co.nz/insights/biometric-processing-privacy-code-now-in-force

- **Dentons** – New Zealand's Privacy Commissioner issues Biometric Processing Privacy Code.
  https://www.dentons.co.nz/en/insights/articles/2025/august/8/new-zealands-privacy-commissioner-issues-biometric-processing-privacy-code

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

P.I.A.

Privacy Impact Assessment: Implementation of a Biometric Time-Tracking System – New Zealand | 2025 Version

Organisation Name	
Contact Person	
Date of Assessment	
Version Number	
Assessor(s)*	

* This can be a project manager, HR lead, operations coordinator, privacy officer, or any staff member familiar with the system and its risks. External legal advice is recommended for high-risk implementations but not required.

1. Description of Proposal

Purpose and Objectives:
State what the organisation hopes to achieve (e.g., accuracy of attendance records, reduction of time fraud, etc.).

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

1. (continued)... **Description of Proposal**

Scope:
Describe who and what is covered: employees, contractors, sites, or business units.

Stakeholders:
List key people involved (project lead, HR, IT, privacy officer, vendor).

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

2. Legal and Policy Context

Identify the relevant laws, codes and internal policies:

✓/X

- [ ] Privacy Act 2020
- [ ] Biometric Processing Privacy Code 2025
- [ ] Employment Relations Act 2000
- [ ] Organisations' internal privacy, security, and employment policies

Indicate if any exemptions or special authorisations apply:

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

3. Information Flows

- **What biometric data will be collected?**

  Digital, analog or algorithmic representations of:

☐ Fingerprints	☐ Palm / hand geometry
☐ Facial geometry	☐ Face photos
☐ Iris/eye scans	☐ Voice recognition
☐ Vein mapping	☐ Video-feed recognition
☐ Other:	

- **In what format will the biometric data be captured?**

A. Raw samples

- ☐ Raw image (e.g., JPEG/PNG/TIFF)
- ☐ Fingerprint image (e.g., WSQ,JPEG2000)
- ☐ Raw audio (e.g., WAV)
- ☐ Video (e.g., MP4,MOV)
- ☐ 3D/depth data (e.g., point cloud/mesh)

B. Processed Representations (templates / embeddings)

- ☐ Standardised template (ISO/IEC 19794-x; e.g., fingerprint minutiae)
- ☐ Proprietary vendor template/embedding
- ☐ Feature vector only (model embedding)
- ☐ Cancelable/transform-protected template (non-invertible transform)

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

C. Derived signals / metadata (no raw biometrics)

- ☐ Quality/liveness scores only
- ☐ Match score/decision only (no template retained)
- ☐ Cryptographic sketch/fuzzy extractor data
- ☐ Pseudonymous identifier derived from biometric

D. Packaging / encoding at capture

- ☐ Encrypted on device at capture (e.g., secure element/TEE)
- ☐ Digitally signed/attested sample (e.g., FIDO2/WebAuthn attestation)
- ☐ Tokenised before transmission/storage

E. Other

- When will Biometric data be collected?
  - ☐ One-time enrollment / registration
  - ☐ At each authentication / sign-in
  - ☐ Periodic re-verification (e.g., quarterly, annually)
  - ☐ Continuous/ongoing monitoring while service is in use
  - ☐ Event-triggered (e.g., alarm, high-risk action, custody transfer)
  - ☐ Ad-hoc/manual (operator-initiated as needed)
  - ☐ Bulk import from another system (provide source):

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

- How will it be collected? (method, device, environment)
  - ☐ Fingerprint scanner (optical)
  - ☐ Fingerprint scanner (capacitive/ultrasonic)
  - ☐ Face camera (2D/RGB)
  - ☐ Face camera with IR/3D depth
  - ☐ Iris scanner
  - ☐ Palm/vein scanner
  - ☐ Voice via microphone/IVR
  - ☐ Signature pad / stylus tablet
  - ☐ Behavioral sensors (e.g., keystroke, gait via camera)
  - ☐ Mobile device sensors (phone/tablet)
  - ☐ Self-service kiosk/terminal
  - ☐ Desktop/laptop webcam
  - ☐ CCTV / fixed surveillance camera (clearly signed)
  - ☐ Remote capture via web browser (e.g., WebAuthn)
  - ☐ Third-party SDK/app integrated into our service
  - ☐ Liveness/spoof detection used (passive)
  - ☐ Liveness/spoof detection used (active challenge)
  - ☐ Other device/method (specify): _____

- Where will collection occur?
  - ☐ On-site at organisation premises
  - ☐ Remote / at home (user's device)
  - ☐ In the field (mobile workforce)
  - ☐ Third-party/partner premises (name): _____
  - ☐ Publicly-accessible area with posted notice
  - ☐ Other location: _____

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

- By whom will it be collected? (role/party)
  - ☐ End user self-capture (unsupervised)
  - ☐ End user self-capture (supervised)
  - ☐ Trained operator/attendant (employee/contractor)
  - ☐ Security/reception staff
  - ☐ Call-center/IVR system (automated)
  - ☐ Automated system/service (no human present)
  - ☐ Third-party processor/vendor (name): _____
  - ☐ Law-enforcement request (legal basis recorded)

- Additional controls at collection
  - ☐ Alternative / non-biometric option offered (**required**)
  - ☐ Consent obtained
  - ☐ Age / guardian checks (if minors may be captured)
  - ☐ Accessibility accomodations available
  - ☐ Cultural accomodations available

- Where will the biometric data be stored? (tick all that apply)
  - ☐ New Zealand only (single-region)
  - ☐ Inside NZ – on device (secure element/TEE)
  - ☐ Inside NZ – on-premise (data centre: _____)
  - ☐ Inside NZ – cloud region (provider/region: _____)
  - ☐ Outside NZ – single country (country: _____, provider: _____)
  - ☐ Outside NZ – multi-region
    (list regions/countries: _____)
  - ☐ Global/"multi-tenant" region chosen by vendor (no data-residency guarantee e.g. wherever the provider's servers and backups are located)

Privacy Impact Assessment

- **Specific common regions (if applicable)**
  - ☐ New Zealand
  - ☐ Australia (e.g., Sydney/Melbourne)
  - ☐ Singapore
  - ☐ EU (e.g., Ireland/Frankfurt/Netherlands)
  - ☐ United Kingdom
  - ☐ United States (state(s): _____)
  - ☐ Other: _____

- **Secondary copies & movement**
  - ☐ Backups in New Zealand
  - ☐ Backups outside New Zealand
  - ☐ Disaster recovery (DR) site in NZ
  - ☐ DR site outside NZ (country/region: _____)
  - ☐ CDN/edge caches (list countries if biometric content ever cached) (where cached: _____)
  - ☐ Logs/telemetry containing biometric identifiers (where stored: _____)

- **Storage scope**
  - ☐ Production only
  - ☐ Non-production (dev/test/staging)
  - ☐ Analytics/data lake
  - ☐ Long-term archival
  - ☐ On-device (hardware/mobile)
  - ☐ Local network appliances (on-premise PC/laptop/server)
  - ☐ Remote network or cloud appliances (AWS/Azure/Vendor servers)

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

- Will it be shared or processed by any third parties?

A. Overall stance

- [ ] No third-party sharing/processing (processors, vendors, affiliates, none)
- [ ] Yes — third parties involved (list each vendor/recipient + purpose):

B. Data elements shared

- [ ] Raw biometric samples
- [ ] Biometric templates/embeddings (non-invertible)
- [ ] Match scores/decisions only
- [ ] Liveness/quality scores only
- [ ] Pseudonymous identifiers only
- [ ] Aggregated/de-identified data
- [ ] Metadata/logs that could indirectly identify individuals

C. Sharing flow & location

- [ ] On-shore (New Zealand) only
- [ ] Cross-border transfers (list countries/regions):

- [ ] Onward sharing by vendor prohibited by contract
- [ ] Onward sharing permitted (list conditions/recipients):

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

D. Role & purpose (per third party)

- [ ] Data processor (operational processing on our behalf)

  Acts only on our documented instructions to handle biometric data for our purposes (Privacy Act "agent/processor" role).

- [ ] Sub-processor of a primary vendor

  A downstream provider engaged by our main vendor to perform part of the processing, under equivalent contractual safeguards.

- [ ] Joint controller / independent controller

  Joint controller: decides purposes/means together with us. Independent controller: decides its own, separate purposes/means.

- [ ] Identity verification / KYC

  Uses biometric data to confirm a person's identity to meet onboarding or AML/CFT obligations.

- [ ] Authentication / access control

  Uses biometric factors to grant/deny user access to systems, apps, or facilities.

- [ ] Liveness/anti-spoof analysis

  Detects presentation attacks (photos, masks, replays) to confirm a real, present person.

- [ ] Model training/improvement (vendor) — explicit approval required

  Vendor uses biometric data or derivatives to train/improve its algorithms; only allowed with our explicit, recorded consent and safeguards.

- [ ] Support/maintenance (ticket, debug, telemetry)

  Limited, purpose-bound access to data (or redacted samples/metadata) to resolve issues and maintain service reliability.

- [ ] Storage/backup/DR provider

  Hosts encrypted data, backups, or disaster-recovery replicas under our retention/location requirements.

- [ ] Analytics/quality metrics (de-identified)

  Produces stats or QA signals using de-identified/aggregated data with no reasonable re-identification risk.

- [ ] Law-enforcement/regulated disclosure (legal basis recorded)

  Discloses data only when legally required or permitted (e.g., warrant/ statutory duty), with the legal basis documented (IPP11).

- [ ] Other purpose:

Privacy Impact Assessment

E. Legal & contractual safeguards

- [ ] **DPA in place with third party (attach ref)**

  A signed Data Processing Agreement with any vendor handling your biometric data, citing the legal basis, roles, and safeguards (attach the contract reference/URL or file ID).

- [ ] **Sub-processor list reviewed/approved**

  You've checked and okayed the vendor's downstream providers (hosting, analytics, support, etc.) that may access biometric data, and you keep a current list.

- [ ] **Cross-border mechanism recorded (e.g., SCCs/IDTA/adequacy/consent)**

  For any overseas disclosure, you've documented the transfer safeguard—e.g., EU SCCs, UK IDTA, NZ "comparable privacy safeguards"/adequacy, or explicit, informed consent.

- [ ] **Purpose limitation & data minimisation contractually enforced**

  The contract limits use of biometric data to the stated purposes only, and requires collecting/keeping the minimum necessary.

- [ ] **Processing limited to documented instructions**

  The vendor may process biometric data only as you (the controller/agency) have written in the DPA/SOW—no unilateral repurposing.

- [ ] **Audit/inspection rights granted**

  You have contractual rights to audit or obtain independent audit reports (e.g., ISO 27001/SOC 2) to verify compliance and controls.

- [ ] **Incident notification SLA defined (___ hrs)**

  The contract sets a deadline (e.g., 24/48 hours) for the vendor to notify you after becoming aware of a suspected or actual breach/security incident involving biometric data.

- What is the retention period (list each destination/third-party)

Party / Destination	Retention Period

4. Purpose, Necessity and Proportionality Assessment

- Purpose for collection of biometric information

  Organisations must only collect biometric information if they can meet all the below conditions:

☐ The collection is for a lawful purpose.

Lawful purpose examples:
Time-tracking for payroll calculation (PAYE/Holidays Act entitlements), attendance verification.

Unawful or likely unlawful purpose examples:
"Productivity-scoring", marketing or sales profiling, monitoring certain activities, covert or surprise collection (no notice, no signage, hidden cameras), off-duty tracking, open-ended "research/analytics".

☐ The collection is **necessary**.

Necessary includes that it is effective and **there are no reasonable alternatives with less privacy risk**.

☐ Have implemented appropriate privacy safeguards.

☐ The biometric processing is proportionate to the likely impacts on people.

. • Describe your lawful **purpose.**

. • Describe why biometrics are **necessary** and **effective** for this purpose.

Privacy Impact Assessment

- Which less intrusive time docking alternatives did your organisation assess?
  - ☐ Key Tag / Swipe Card
  - ☐ PIN code
  - ☐ Self check-in (mobile/kiosk/PC/paper)
  - ☐ Punch card
  - ☐ Manual entry (incl. manual reporting e.g. email/SMS)
  - ☐ Other: _____

- Why less obtrusive alternatives were rejected:

- How was privacy impact and cultural effect (incl. on Māori) considered?

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

- If running a trial, note the duration and evaluation plan:

  Duration:

  Evaluation Plan:

5. **Collection and Transparency**

   Describe how individuals will be informed before collection.

   - How will you inform individuals of what data is being collected and why?

   - How will you inform individuals of who will hold and access it?

- How will you inform individuals of whether/which alternatives are available?

- How will you inform individuals of how long will data be retained?

- How will you inform individuals of any consequences of not providing data?

- How will you inform individuals of their rights of access, correction, and complaint (to the Privacy Commissioner or internal contact)?

- When will you inform individuals? (e.g. pre-employment, attached with job offer / acceptance letter, etc.)

Privacy Impact Assessment

6. **Key Privacy Risks and Safeguards**

☐ Employees are informed before collection (what data, why, how stored, access, and alternatives).

Risk	Severity	Mitigation / Safeguard	Mitigated Severity
Over-collection Collecting more biometric data than required.	Medium		
Data breach Unauthorised access or use of biometric data.	High		
Function creep Using data beyond time-tracking (for the stated purpose).	High		
Employee choice Feeling coerced or unable to opt out.	Medium		
Cultural impact Objection based on personal values or beliefs.	Medium		
Accuracy errors False accepts/rejects causing access/pay errors.	Medium		
Algorithmic bias Higher error rates for certain demographics.	Medium		
Faked / spoofing Attempts with masks, photos, "gummy" fingers.	Medium		

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

Risk	Severity	Mitigation / Safeguard	Mitigated Severity
Over-collection Collecting more biometric data than required.	Medium		
Insecure storage Templates or keys exposed due to weak storage/ops.	High		
Cross-border transfers Vendor replicates data offshore without safeguards.	High		
Duplication Templates used to match staff elsewhere.	High		
Retention creep Data kept longer than necessary.	Medium		
Weak transparency Staff can't access/correct information easily.	Medium		
Lock-in / portability Can't migrate or securely erase on exit (from vendor).	Medium		
Monitoring creep Use outside work/time/location; covert performance monitoring.	High		
Physical tampering Devices tampered with or stolen.	Medium		
Hygiene / infection risk Shared sensors (e.g., fingerprint) transmit germs.	Low		

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Privacy Impact Assessment

Risk	Severity	Mitigation / Safeguard	Mitigated Severity
Power/network outage Payroll impact. Staff can't clock; pay disputes.	Medium		
Misconfiguration Default credentials, exposed ports, weak Wi-Fi or passwords.	High		
Enrollment bottlenecks Queues, frustration, minor H&S issues.	Low		
Accessibility failure People unable to use modality (injury/disability).	Medium		
Non-compliance Breach of privacy/biometrics code or labor law.	High		
Third-party risk Installer/support staff mishandle data/devices.	Medium		
Disposal leakage Data left on devices/media at end-of-life.	High		

7. **Best-effort put forward**

☐ Mitigations and safeguards have been thouroughly assessed, discussed with all individuals and presented for feedback and improvement.

Sign-off & Review

By signing below, the undersigned confirms that all agreed processes and controls in this Privacy Impact Assessment have been implemented, residual severities are acceptable, and supporting evidence (policies, configurations, training records, vendor assurances, and deletion/rollback plans) are on file.

They acknowledge roles and escalation paths, including an equivalent non-biometric alternative for anyone who opts out, and commit to maintaining access reviews, patching, and audit logging.

Any outstanding actions are recorded with an owner and due date, and payroll assurance and incident response playbooks have been tested.

This P.I.A. will be reviewed after the first month in production, then at least annually—or sooner following any material change (new modality, vendor, location, or purpose), significant incident, or audit finding.

Overall Impact	Low / Medium / High
Role	
Date	
Signature	

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Not for production use
Example / Demonstration only

Employee Consent Form

*This is an example form, intended to be curated by your organisation and relevant advisors, based on the policies you wish to implement.

Employee Biometric Time-Tracking Information and Acknowledgment Form

Purpose of collection

[Organisation Name] uses biometric identification for the purpose of time-tracking [to record employee attendance accurately and reduce time-recording errors or misuse].

Type of information collected

We will collect and store a [digital biometric template (for example, a fingerprint or facial recognition template)].

The system does **not** store raw images or photos — only an encrypted numerical template.

Use of information

Biometric data will be used **only** to verify your identity [when clocking in or out / switching tasks].

It will **not** be used for monitoring, profiling, or any unrelated purpose.

Storage and security

All biometric templates are encrypted and stored securely in New

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made

Not for production use

Example / Demonstration only

Storage and security

All biometric templates are encrypted and stored securely in New Zealand. Only authorised system administrators may access this information.

Retention and deletion

Your biometric data will be deleted when you leave employment or when the biometric system is no longer required.

Your options

You may choose whether or not to use the biometric method.

If you do not wish to use it, you may use an approved alternative time-recording method (such as PIN, swipe card, or mobile app).

Please tick one option

☐ **I prefer not to use biometrics** and request an alternative method for recording attendance or hours of work.

☐ **I consent** to the collection and use of my biometric information for time-tracking purposes as described above.

Name	
Date	
Signature	

TIMEDOCK

NZBN
9429030761612

Incorporated
NZ owned & privately held. 2012.

Contact
info@timedock.com
(07) 808 1203

Headquarters
4/144 Third Avenue
Tauranga 3110
New Zealand

Website
https://timedock.com

New Zealand Made