



Privacy Policy

For the TAU scanner app, grower dashboard, website, AI processing, support and related services

Effective date	18 July 2026
Version	1.0
TAU legal entity	TAU Research Limited trading as TAU / TAU Research
Privacy contact	Unit 5, 4 Hammond Street, Hamilton Central, Hamilton, 3204, New Zealand rh.innovationltd@gmail.com NZBN 9429048619677

PRIVACY AT A GLANCE

Tau collects account, business, orchard-scanning, location, device and usage information to provide and secure the Services, process scans, support users, bill customers, and improve our technology. We do not sell personal information. We disclose it only as described in this Policy, including to authorised users, service providers, and where required or permitted by law.

Contents

- 1. About this Policy and who we are
 - 2. Who this Policy applies to
 - 3. Personal information we collect
 - 4. How we collect personal information
 - 5. Why we collect and use personal information
 - 6. Scan data, AI processing and service improvement
 - 7. Cookies, analytics and automatic collection
 - 8. When we disclose personal information
 - 9. Overseas processing and storage
 - 10. Security and privacy breaches
 - 11. Retention and deletion
 - 12. Access, correction and other choices
 - 13. Communications and marketing
 - 14. Children and incidental collection
 - 15. Third-party services and links
 - 16. Changes to this Policy
 - 17. Contact and complaints
- Schedule 1 - Information categories and primary purposes

Plain-language summary

This Policy explains what personal information Tau collects, where it comes from, why we use it, who may receive it, how long we keep it, and how individuals can request access or correction. It should be read with the TAU Terms and Conditions. The Terms govern Customer Data and use of the Services; this Policy governs personal information.

1. About this Policy and who we are

- 1.1** This Privacy Policy explains how TAU Research Limited, trading as TAU / TAU Research ("Tau", "we", "us" or "our"), collects, holds, uses and discloses personal information in connection with the Services.
- 1.2** The Services include the TAU scanner application, grower dashboard, website, AI and data-processing services, support, communications, integrations and related services.
- 1.3** We handle personal information under the New Zealand Privacy Act 2020 and its information privacy principles. Where another law applies, we will also comply with that law to the extent required.
- 1.4** Not all orchard or business data is personal information. Data is personal information where it is about an identifiable individual. Customer Data that is not personal information is governed by the TAU Terms and Conditions and any applicable Order Form or data-sharing agreement.
- 1.5** Some information is required to create an account, process a scan, provide Results, secure the Services, meet legal obligations or administer payment. If required information is not supplied, we may be unable to provide some or all of the Services. Optional information will generally be identified as optional or can be omitted without preventing the core service.

2. Who this Policy applies to

- 2.1** This Policy applies to individuals who use or interact with Tau, including growers, orchard owners, authorised users, orchard managers, packhouse staff, contractors, drivers, employees of customer organisations, website visitors, prospective customers, suppliers and support contacts.
- 2.2** Where a business or organisation supplies personal information about its personnel, growers, contractors or other individuals, that organisation must have authority to provide it and must take reasonable steps to ensure those individuals are aware of this Policy, unless an exception applies.
- 2.3** If you use an account supplied by an employer, packhouse, orchard manager or other organisation, that organisation may control your access and may be able to view account activity, scan data, Results and video previews associated with its account. Its own privacy practices may also apply.

3. Personal information we collect

- 3.1** Account and identity information, such as name, email address, phone number, job title, organisation, user ID, login credentials, authentication information and account permissions.
- 3.2** Customer and business information, such as billing contacts, orchard ownership or management relationships, site and block names, orchard address or location, packhouse, crop variety, area, quotes, subscriptions, invoices and payment status.
- 3.3** Scanning and field information, such as video, images, GPS coordinates and tracks, timestamps, row width, row height, bay length, scan stage, lens settings, camera and brightness settings, device orientation, manual counts, field notes, crop records, validation information and packout-related information supplied to us.
- 3.4** Device, usage and security information, such as IP address, device model, operating system, browser, app version, mobile network, session identifiers, login history, upload status, diagnostics, crash logs, performance data, audit records and security events.
- 3.5** Communications and support information, such as emails, support requests, call notes, feedback, survey responses, complaints and records of interactions with us.
- 3.6** Transaction information, such as products or services purchased, invoice details, payment method type and payment status. If we use a third-party payment processor, that provider may collect full payment-card or bank details directly under its own privacy policy; Tau may receive only limited transaction information.
- 3.7** Incidental information within recordings. Orchard scans are intended to capture the canopy and crop. A recording may nevertheless incidentally include a person, voice, vehicle registration, neighbouring property or other identifiable information, depending on the environment and device settings.

4. How we collect personal information

- 4.1** Directly from you when you create or use an account, enter field information, record or upload a scan, contact support, request a quote, pay an invoice, provide feedback, complete a form or communicate with us.

- 4.2 Automatically from the app, dashboard, website, devices and technical systems when you log in, scan, upload, process data, view Results or otherwise use the Services.
- 4.3 From your organisation or another authorised source, such as an employer, orchard owner, grower, packhouse, orchard manager, contractor, account administrator, referral partner or another authorised user.
- 4.4 From service providers and integrations, such as identity, hosting, storage, communications, analytics, payment, support and security providers, where needed to operate the Services.
- 4.5 From publicly available business sources where reasonably necessary, such as company registers, business websites, directories and professional contact information.
- 4.6 When we collect personal information about an individual from another source, we will take reasonable steps to make the individual aware of the collection and the matters required by law, unless the individual is already aware or another legal exception applies.

5. Why we collect and use personal information

- 5.1 To create, verify, administer and secure accounts, authenticate users, manage permissions and provide the Services requested by the customer.
- 5.2 To receive, store, organise and process scans and Customer Data; generate counts, density estimates, heatmaps, summaries, insights, forecasts, video previews and other Results; and make those Results available to authorised users.
- 5.3 To provide onboarding, documentation, technical support, troubleshooting, training and service communications.
- 5.4 To prepare quotes, administer subscriptions, issue invoices, process payments, recover debts and maintain tax, accounting and business records.
- 5.5 To monitor service quality and performance, investigate errors, prevent misuse and fraud, protect users and systems, enforce the Terms, and maintain technical and audit records.
- 5.6 To analyse and improve the Services, test and evaluate models, develop new features, conduct research, understand usage patterns and improve scanning guidance and user experience.
- 5.7 To communicate about service updates, security, product changes, training, events and relevant Tau products or services, subject to applicable communication and marketing rules.
- 5.8 To comply with law, respond to lawful requests, establish or defend legal claims, manage insurance, conduct due diligence and protect Tau, customers, individuals and the public.
- 5.9 For another purpose authorised by you, directly related to the purpose of collection, or otherwise permitted by law.

6. Scan data, AI processing and service improvement

Important

Tau AI is designed to analyse orchard items and crop conditions, not to evaluate individuals. Results are crop estimates and decision-support outputs. They are not used by Tau to make solely automated decisions about an individual that produce legal or similarly significant effects.

- 6.1 We process scan videos, images, GPS, measurements, device data and related metadata to generate Results and provide quality checks, previews, maps and analytics.
- 6.2 We may use Customer Data and associated personal information for quality assurance, troubleshooting, model evaluation, model improvement, product development and research where this is reasonably necessary to provide and improve the Services and is permitted by the agreement and law.
- 6.3 Where reasonably practicable, we minimise, aggregate or de-identify personal information before using data for analysis, benchmarking, model improvement or research. We may retain and use aggregated or de-identified information that no longer reasonably identifies an individual for legitimate business purposes.
- 6.4 Users should avoid deliberately filming people, private areas or unrelated neighbouring property, and must obtain any permissions required by the Terms and applicable law. If you believe a recording contains unnecessary personal information, contact us promptly and identify the relevant scan or file.
- 6.5 Authorised users associated with the customer account may be able to view scan previews, maps, Results and related metadata. Customers are responsible for assigning access only to appropriate personnel and promptly removing access when it is no longer required.

7. Cookies, analytics and automatic collection

- 7.1 The dashboard and website use essential cookies or similar technologies to support login, security, session management, preferences and core functionality.

- 7.2** We may use analytics and diagnostic technologies to understand how the Services are used, identify errors, measure performance and improve usability. These technologies may collect device, browser, IP address, page, event and session information.
- 7.3** You can control cookies through your browser or device settings. Disabling essential cookies may prevent login or cause parts of the Services to stop working. Where consent is legally required for a non-essential technology, we will request it through an appropriate notice or control.

8. When we disclose personal information

- 8.1** Within Tau, to personnel and contractors who need the information to perform their roles and who are subject to confidentiality and security obligations.
- 8.2** To service providers that help us host, store, process, secure, analyse, communicate, bill, support or maintain the Services. Providers may use personal information only for the services they provide to us or as otherwise permitted by law and their agreements with us.
- 8.3** To the customer organisation and its authorised users, administrators, growers, orchard owners, packhouses, orchard managers, advisers, contractors or integration partners where the customer has directed or authorised the sharing, or where it is reasonably necessary to provide the Services.
- 8.4** To professional advisers, auditors, insurers, financiers and prospective buyers or investors where reasonably necessary for advice, insurance, financing, a business transaction or due diligence, subject to appropriate confidentiality protections.
- 8.5** To courts, regulators, law enforcement, government agencies or other persons where required or permitted by law, or where reasonably necessary to protect safety, rights, property, systems or the public.
- 8.6** With your authorisation or at your direction, including through an API, portal, export, integration or data-sharing arrangement.
- 8.7** We do not sell personal information or identifiable orchard-level Customer Data for third-party advertising or marketing. We may share aggregated or de-identified information that does not reasonably identify an individual or specific customer, subject to the Terms and any applicable agreement.

9. Overseas processing and storage

- 9.1** Tau is based in New Zealand, but some service providers or their systems may be located outside New Zealand. This means personal information may be processed or stored in another country.
- 9.2** Before disclosing personal information to an overseas recipient, we will take reasonable steps to ensure it is protected in a way that provides safeguards comparable to the New Zealand Privacy Act, or we will rely on another basis permitted by law. This may include contractual protections, due diligence, security controls, or confirming that the recipient is otherwise subject to appropriate privacy obligations.
- 9.3** An overseas provider may be subject to the laws of its country and lawful access requests from authorities there. You may contact our Privacy Officer for more information about the categories of overseas providers used for the Services.

10. Security and privacy breaches

- 10.1** We use reasonable administrative, technical and organisational safeguards appropriate to the nature of the information and the risks involved. Measures may include access controls, authentication, encryption, secure hosting, backups, monitoring, staff or contractor confidentiality obligations and incident-response processes.
- 10.2** No mobile, internet, cloud or storage system can be guaranteed completely secure. You must protect account credentials, use supported and updated devices, control access within your organisation and notify us promptly of suspected unauthorised access or loss.
- 10.3** If a privacy breach has caused or is likely to cause serious harm, we will notify the Office of the Privacy Commissioner and affected individuals as soon as practicable, unless a legal exception applies. We may also contact customers or users to contain, investigate and reduce the effects of an incident.

11. Retention and deletion

- 11.1** We retain personal information only for as long as reasonably required for the purposes for which it may lawfully be used, including providing the Services, maintaining security and audit records, supporting customers, meeting contractual commitments, resolving disputes and complying with tax, accounting and legal obligations.
- 11.2** Retention periods vary by information type, account status, customer instructions, technical architecture, legal requirements and the applicable Order Form. Customers should export any Customer Data or Results they need before account closure or expiry of an agreed retention period.
- 11.3** After information is no longer required, we may delete, anonymise or de-identify it. Deletion from active systems may not immediately remove information from secure backups, which are overwritten or deleted through normal backup cycles.

- 11.4** We may retain aggregated or de-identified data, model improvements, security logs and records that do not reasonably identify an individual, subject to law and the agreement.

12. Access, correction and other choices

- 12.1** An individual may ask whether we hold personal information about them and request access to it. The right applies to personal information about the individual, not necessarily all business, orchard, confidential, evaluative or third-party information held in the same record.
- 12.2** An individual may ask us to correct personal information they believe is inaccurate. If we do not make the requested correction, the individual may ask us to attach a statement of correction to the information where required by law.
- 12.3** Requests should be sent to our Privacy Officer at rh.innovationltd@gmail.com. We may ask for information to verify identity, authority and the scope of the request. We will respond within the time required by law and may withhold information only where a lawful ground applies.
- 12.4** You may update some account details through the Services or through your account administrator. You may also ask us to close an account, subject to outstanding payment, legal retention and customer-organisation requirements.
- 12.5** Where processing depends on your authorisation, you may withdraw that authorisation for future processing, but this will not affect processing already carried out and may prevent us from providing part or all of the Services.

13. Communications and marketing

- 13.1** We may send operational messages necessary to provide the Services, such as account, upload, processing, security, billing, support and material service-change notices. These messages are not optional while the relevant account or service remains active.
- 13.2** We may send information about Tau products, training, events or offers where permitted by law. You can opt out of marketing messages using the unsubscribe method in the message or by contacting us. Opting out of marketing does not stop operational communications.

14. Children and incidental collection

- 14.1** The Services are intended for business users who are at least 18 years old and are not directed to children.
- 14.2** A scan may incidentally capture a child or other person present in an orchard. Users should avoid unnecessary capture and follow property, safety, consent and privacy requirements. If we learn that unnecessary personal information about a child has been collected, we will assess appropriate restriction, deletion or other action.

15. Third-party services and links

- 15.1** The Services may link to or integrate with third-party websites, devices, payment services, app stores, mapping tools, packhouse systems or other platforms. Those third parties control their own privacy practices, and their privacy policies apply to information they collect directly.
- 15.2** Tau is not responsible for a third party's privacy or security practices except to the extent Tau is legally responsible for selecting or managing that provider in connection with the Services.

16. Changes to this Policy

- 16.1** We may update this Policy to reflect changes in law, technology, providers, data practices or the Services. The current version will show its effective date and version number.
- 16.2** Where a change is material, we will take reasonable steps to notify affected users or customers before or when it takes effect, unless an earlier change is required for legal, security or operational reasons.
- 16.3** If a proposed new use of personal information requires additional notice or authorisation under law, we will provide that notice or obtain that authorisation as appropriate rather than relying only on an updated Policy.

17. Contact and complaints

- 17.1** Privacy Officer: TAU Research Limited. Email: rh.innovationltd@gmail.com. Postal address: Unit 5, 4 Hammond Street, Hamilton Central, Hamilton, 3204, New Zealand. NZBN: 9429048619677.
- 17.2** Please contact our Privacy Officer first if you have a privacy question, request or complaint. Include enough information for us to understand the issue, but do not email passwords or unnecessary sensitive information.
- 17.3** If you are not satisfied with our response, you may make a complaint to the New Zealand Office of the Privacy Commissioner through [privacy.org.nz](https://www.privacy.org.nz). The Commissioner may ask you to raise the matter with us first.

Schedule 1 - Information categories and primary purposes

How to read this table

The examples below are not exhaustive. The exact information collected depends on the features used, the customer arrangement, device settings and the scan workflow.

Category	Examples	Primary purposes
Account and identity	Name, email, phone, role, organisation, user ID, credentials, permissions	Account creation, authentication, access control, support, security and communications.
Business and billing	Orchard or organisation details, contacts, quote, subscription, invoice and payment status	Customer administration, contracting, billing, payment, tax and business records.
Scan and field data	Video, images, GPS, timestamps, site, block, dimensions, crop stage, settings, field notes and supplied validation data	Scan processing, Results, maps, quality checks, previews, troubleshooting and service improvement.
Device and usage	IP address, device model, OS, browser, app version, sessions, logs, crashes and diagnostics	Functionality, performance, security, fraud prevention, analytics and support.
Communications	Support emails, feedback, surveys, complaints and interaction records	Support, issue resolution, service improvement, relationship management and legal records.
Incidental recording content	People, voices, vehicles, registrations or neighbouring property captured unintentionally	Providing the scan service, quality review, investigating a reported issue and deletion or restriction where appropriate.
Derived and de-identified data	Quality scores, usage metrics, aggregated statistics, de-identified scan features and model evaluation outputs	Model improvement, research, benchmarking, product development, capacity planning and business analysis.

TAU contact details

Legal entity	TAU Research Limited
Trading name	TAU / TAU Research
NZBN	9429048619677
Registered address	Unit 5, 4 Hammond Street, Hamilton Central, Hamilton, 3204, New Zealand
Privacy Officer	rh.innovationltd@gmail.com

End of Privacy Policy