

Privacy Policy

Version 2026.1 · Effective 12 October 2026

This policy explains how **Unicloud Limited** (New Zealand company number 6762413, "we", "us") handles personal information under the Privacy Act 2020. It applies to all our websites, software, apps and services, under our own name or a product name. It sits alongside our Terms of Service and, for business customers, our Data Processing Addendum.

1. Whose information, and who is responsible for it

If you are...	Who is responsible for your information
A visitor to our websites, a business contact, supplier or job applicant	We are. This policy applies in full.
A user of our software through an organisation (your employer, contractor, flight school, franchise or client)	That organisation is. It puts your information into the software and decides how it is used. We hold it for them as their agent under section 11 of the Privacy Act 2020, and use it only to run the software for them. Their privacy statement applies, and this policy explains how we protect it. Your sign-in and security records (section 2) are covered by this policy too.

If you want to see or correct information an organisation holds about you in our software, ask that organisation first. If you contact us, we will pass your request to them within 5 working days and help them answer it.

2. What we collect and why

Who	What we collect	Why
Website visitors	What you type into a contact or demo form. Our web servers log your IP address, browser and the pages requested.	To reply to you, and to keep the websites running and secure.
Business contacts	Name, role, work email and phone, billing details, and our correspondence.	To set up and run the services, invoice, support you, and tell you about changes.
Users of any of our software	Your login email and name, sign-in times, IP address, device and browser, approximate location derived from your IP address (city and country), security events, and support requests or feedback you send us (which may include a screenshot or a short screen recording if you choose to attach one).	To secure Accounts, detect misuse, investigate problems and support you.
Suppliers and contractors	Contact, bank and tax details; for our own contractors, what we need to engage them and give them system access.	To engage and pay them and manage access.
Job applicants	Your CV and what you tell us; referee comments with your permission.	To assess your application.

We collect only what we need for these purposes. You can choose not to give us information, but we may then be unable to provide a service or reply to you.

Sensitive information

Organisations using our software may record more sensitive information about their people, such as medical certificate details, injury reports, identity documents or student numbers. They are responsible for that information under section 1, and we protect it under our Data Processing Addendum.

Young people

Our services are for organisations and are not directed at children. Organisations may record information about trainees or staff under 18 in our software; they are responsible for it and must take particular care, as information privacy principle 4 requires.

Information we get from someone else

Sometimes we receive your details from another person, for example a customer naming you as its billing contact, or a referee. Where we collect information this way for our own purposes, we take reasonable steps to tell you, as information privacy principle 3A requires, unless an exception applies (for example you already know).

3. Cookies and tracking

We use only the cookies and browser storage needed to sign you in, keep forms secure, and remember your settings. We do not use advertising or cross-site tracking cookies, and our websites do not use third-party analytics. Our software keeps its own records of which pages are used, to improve the software and support you; these are not shared with advertisers.

4. Marketing

We send product news only to business contacts and to people who have asked for it. Every marketing email says it is from us and has an unsubscribe link that works within five working days, as the Unsolicited Electronic Messages Act 2007 requires. Service messages (security, billing, renewal and change notices) are not marketing, and you will receive them while you have an Account.

5. AI features

Some features use Google's Gemini API, and one business feature uses Anthropic. When you use one of these features, the information it needs (which may include text, photos or documents) is sent to the provider to produce the result. Before sending, features built to reason about people replace names held in name fields with placeholders and remove email addresses, phone numbers and long identifying numbers from free text. We do not use your information to train AI models, and our providers' terms for the paid services we use prevent them from doing so. Google keeps requests for up to 55 days to detect abuse of its service, and Anthropic for up to 30 days. We keep the result where it becomes part of your records (for example a summary or a label). We do not otherwise keep the text of requests and answers, except where an organisation's administrator chooses to keep it (up to 90 days), or a short excerpt where a security check flags a request (90 days).

6. Who we share it with

We do not sell personal information. We share it only with the service providers below, who process it for us under contract; with our professional advisers, insurers and bank where needed; with a buyer of our business under a confidentiality agreement; or where the law requires it, or the Privacy Act 2020 permits it (for example to prevent a serious threat to someone's safety).

Provider	What it does for us	Where processed
----------	---------------------	-----------------

All services		
Cloudflare	Domain names, network security, email sending	Global network
SMTP2GO	Email delivery, including website forms	Global network (New Zealand company)
Google	AI features (Gemini), maps, our business email and documents	Global
Xero	Invoicing and accounts	Global (New Zealand company)
Our bank	Payments	New Zealand
Our software		
Railway	Hosting of databases, files and backups	Singapore; United States for our training software
Anthropic	AI for contract review, where a customer uses it	United States
ClickSend	Text messages, where a customer switches them on	Australia
OpenStreetMap Foundation	Address lookup where Google Maps is not set up	United Kingdom / Europe
Railway	The system that runs backups and handles support requests	Netherlands

Business customers get 30 days' notice before we add or replace a provider that handles their data. The current list for each business service is kept in its Security & Compliance section.

7. Information held or processed overseas

Most of our information is stored in Singapore or the United States, as shown above, and some providers process it in other countries. When an overseas provider only stores or processes information for us, we stay responsible for it under the Privacy Act 2020. We choose providers bound by data processing terms that protect information in a way comparable to the Privacy Act, and we encrypt it in transit and at rest.

Our staff in New Zealand and the United Kingdom may access information to provide support. If we ever disclose personal information to an overseas organisation for its own use, we will do so only where information privacy principle 12 allows it.

8. How we protect it

Each business customer has its own database and file store. Information is encrypted in transit and at rest. Staff access is limited to those who need it, uses multi-factor sign-in and is logged, and when support staff sign in as a user to fix a problem, the session is recorded under their own name. Passwords are stored only as secure hashes, and passkeys are supported. Databases are backed up daily and the backups are encrypted. Releases of our business software are security-tested before they reach customers.

9. How long we keep it

Information	How long
Website enquiries that do not lead to work	2 years from the last contact

Web server logs	90 days
Sign-in history and security events	The period set by the organisation's administrator (12 months unless changed), then deleted automatically
AI request text kept by choice of an organisation's administrator, and flagged security excerpts	90 days
Support requests and feedback, including attachments	2 years after the request is closed
Business contact records	While you are a customer, then 7 years
Invoices and accounting records	7 years (Tax Administration Act 1994)
Unsuccessful job applications	12 months, unless you agree to longer
Employee and contractor records	7 years after the engagement ends
Information held for business customers	As agreed with the customer, and deleted under our Data Processing Addendum when the agreement ends

10. Access and correction

You can ask for the personal information we hold about you, and ask us to correct it (information privacy principles 6 and 7). Contact our Privacy Officer. We check who you are before we release or change anything, and respond within 20 working days. If we decline to correct information, you can ask us to attach a statement of the correction you asked for. We do not charge for these requests.

11. Privacy breaches

If a privacy breach involving information we are responsible for has caused, or is likely to cause, serious harm, we will notify the Privacy Commissioner and the people affected as soon as practicable, as Part 6 of the Privacy Act 2020 requires. For information we hold for a business customer, we tell that customer within 72 hours of becoming aware of a breach that affects it, so it can meet its own duties.

12. Australia and the United Kingdom

Where we handle personal information about people in Australia, the Australian Privacy Principles also apply, and you may complain to the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992). Where UK data protection law applies to us, you have the rights it gives, and you may complain to the Information Commissioner's Office (ico.org.uk).

13. Contact us or complain

Privacy Officer: Rob McDonald, Unicloud Limited
Email: admin@unicloud.co.nz (subject: Privacy)
Post: 500 Harvard Lane, Ardmore, Auckland
Phone: 027 742 6915

If you are unhappy with how we have handled your information, please tell us first so we can try to put it right. You can also complain to the Office of the Privacy Commissioner: privacy.org.nz, 0800 803 909.

14. Changes to this policy

We publish each version with a version number and date. We will tell you by email or in the service before a change that affects how we use information you have already given us, and give business customers at least 30 days' notice of a change that affects their data.