

Data Processing Addendum

Version 2026.1 · Effective 12 October 2026

This Addendum forms part of every business agreement under Part B of the Unicloud Terms of Service, whether the customer signed a Schedule of Services or subscribed online. It needs no separate signature. Where it conflicts with the Terms of Service, this Addendum applies. Words defined in the Terms of Service have the same meaning here.

1. Roles

- 1.1** The customer is the agency responsible for Customer Data under the Privacy Act 2020, and the APP entity where the Privacy Act 1988 (Cth) applies. Unicloud holds and processes Customer Data as the customer's agent under section 11 of the Privacy Act 2020, and only on the customer's documented instructions.
- 1.2** The customer's instructions are the Agreement, the customer's use and configuration of the Services, and any further written instruction we agree to. We will tell the customer if we believe an instruction would break the law, and need not follow it.
- 1.3** Where the customer licenses our software to offer under its own brand, it is responsible to its own customers as their provider, and this Addendum applies between us for the data we hold for it.

2. Description of processing

Purpose	Hosting and running the Services for the customer; backups; support; security monitoring; the features the customer chooses to use, including AI features.
People	The customer's staff, contractors, technicians, students, trainees and members, and other people whose details the customer records (for example site contacts or incident witnesses).
Kinds of information	Names, work contact details, roles and logins; site, asset, job, roster, training, licence and qualification records; health and safety reports (which may include injury details); medical certificate details, flight records and logbooks where the customer records them; sign-in times and, where the customer uses on-site sign-in, location at sign-in; uploaded documents and photos; audit logs.
Sensitive information	The Services are not designed for health records beyond the safety, fitness-for-duty and medical-certificate details listed above. The customer should not upload other health, financial or identity documents unless the Schedule of Services provides for it.
Duration	The Term, then until deletion under clause 9.

3. Our obligations

- 3.1** We will:
- (a) use Customer Data only for the purposes in clause 2, and never sell it or use it for our own marketing, profiling, or to train any AI model;
 - (b) keep the security measures in Annex 2 in place, and not reduce their overall level during the Term;

- (c) make sure everyone who can access Customer Data is bound by confidentiality and trained on our security policies, and that access is limited to those who need it;
- (d) keep each customer's data in its own database and file store;
- (e) help the customer respond to requests from individuals to access or correct their information (information privacy principles 6 and 7), and to enquiries from the Privacy Commissioner, within a reasonable time. Help beyond what the Services already let the customer do itself is charged at our hourly rate.

3.2 If we receive a privacy request or complaint about Customer Data directly, we will pass it to the customer within 5 Working Days and will not respond to it ourselves, except to say we have passed it on.

4. Customer obligations

4.1 The customer will:

- (a) collect Customer Data lawfully, and give the people concerned the notices required by information privacy principles 3 and 3A, including that a service provider holds the information for the customer, and in which country;
- (b) take particular care with information about people under 18 (information privacy principle 4);
- (c) set up access groups and site scope so each user sees only what they should, and test that set-up;
- (d) decide which optional features to switch on, including AI features and text messages, and tell its people where its privacy statement requires it.

5. Where data is held

- 5.1** Customer Data is hosted in the country shown for each Service in Annex 1. We will give the customer at least 30 days' written notice before moving it to another country.
- 5.2** Our staff in New Zealand and the United Kingdom may access Customer Data to provide support. They are bound by clause 3.1(c).
- 5.3** Sending Customer Data to our sub-processors for them to process for us is not a disclosure under information privacy principle 12, because they act for us. We remain responsible for them, and we choose providers bound by terms that protect the data in a way comparable to the Privacy Act 2020.
- 5.4** Where the European Union or United Kingdom GDPR applies to the customer's processing, we will sign the relevant standard contractual clauses or UK addendum on request.

6. Sub-processors

- 6.1** The customer authorises the sub-processors listed in Annex 1. The current list is also kept in the Security & Compliance section of each Service.
- 6.2** We will give at least 30 days' written notice before adding or replacing a sub-processor of Customer Data. If the customer reasonably objects on data protection grounds within that period, we will discuss alternatives in good faith. If none is found, the customer may end the affected Services without an early termination charge, and we will refund prepaid fees for the period after termination.
- 6.3** We bind each sub-processor to data protection terms that protect Customer Data at least as well as this Addendum, and remain responsible for what they do with it.

7. AI features

- 7.1 AI features send only the information needed for the task, from the customer's own data and, when a person runs the feature, only from records that person can already see. 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 before sending.
- 7.2 We use only AI providers whose terms prevent them from training on what we send. Annex 1 lists each provider and how long it keeps requests. We do not keep the text of AI requests and answers except where clause A6.4 of the Terms of Service says so.
- 7.3 The customer's administrator can switch AI features off.

8. Security incidents and breaches

- 8.1 We will notify the customer's privacy contact within 72 hours of becoming aware of any unauthorised access to, disclosure, alteration, loss or destruction of Customer Data, or any event that stops the customer accessing it ("Incident"). Our target is 24 hours.
- 8.2 The notice will say what is known at the time: what happened and when, what information and roughly how many people are affected, what we have done to contain it, and who to contact. We will update the customer as we learn more and give it what it needs to assess whether the Incident is a notifiable privacy breach under Part 6 of the Privacy Act 2020 (or an eligible data breach under the Australian scheme).
- 8.3 The customer decides whether and how to notify the Privacy Commissioner and affected people. We will not notify them for the customer unless it agrees or the law requires us to.
- 8.4 We will keep a record of every Incident, and give the customer a written summary of the cause and the steps taken to prevent it happening again within 10 Working Days of resolving it.

9. Return and deletion

- 9.1 During the Term the customer can export its data through the Services, or ask us for a full export.
- 9.2 On request during the Term, we will delete specified Customer Data from the live system within 30 days. The last backup holding it expires within 90 days.
- 9.3 When the Agreement ends, clause B10.5 of the Terms of Service applies: export, then deletion of the live system within 30 days of the customer confirming it has its data, the last backup within 90 days, and written confirmation of what was deleted.
- 9.4 We may keep Customer Data longer only where the law requires it, and then protect it under this Addendum.

10. Audit

- 10.1 Once a year, and after any Incident, the customer may review our compliance with this Addendum: our security documentation, policies and test results, and a walkthrough with our staff. The customer gives 10 Working Days' written notice and signs a confidentiality agreement. Each party pays its own costs. An on-site audit or one by a third-party auditor is by agreement, at the customer's cost.

11. Liability

- 11.1 The limits in clause B9 of the Terms of Service apply to this Addendum, unless the Schedule of Services sets a separate limit for data protection.

Annex 1 - Hosting and sub-processors

As at 12 October 2026. The list in the Security & Compliance section of each Service is updated first and prevails.

Where Customer Data is hosted

Service	Hosting provider	Country
Facilities management software (Facilitease)	Railway (databases, files, backups)	Singapore
Training and learning software (Altivy LMS)	Railway (databases, files, backups)	United States
Backup operations and support system	Railway	Netherlands
Bespoke and legacy client systems	As stated in that client's Schedule of Services	As stated in the Schedule

Sub-processors

Provider	What it does	Where processed	Terms and retention
Railway Corporation	Hosting of databases, files and backups	Countries in the hosting table	Railway DPA. Holds data for as long as we keep it there.
Cloudflare	Domain names, network security, email sending	Global network	Cloudflare DPA. Email content is not stored after delivery.
SMTP2GO	Email delivery	Global network	New Zealand company; Privacy Act 2020 applies directly.
Google (Gemini API)	AI features	Global	Google Cloud DPA; paid-service terms exclude training. Requests kept up to 55 days for abuse monitoring.
Google (Maps Platform)	Maps and address lookup, where used	Global	Google Maps Platform terms. Site addresses and coordinates only.
Anthropic	AI for the contract review feature, where a customer uses it	United States	Anthropic commercial terms and DPA; no training on customer data. Requests kept up to 30 days.
ClickSend	Text messages, only where switched on	Australia	Australian Privacy Act 1988 applies. Mobile numbers and message text.

OpenStreetMap Foundation (Nominatim)	Address lookup where Google Maps is not set up	United Kingdom / Europe	OSMF usage policy. Addresses only.
--------------------------------------	--	-------------------------	------------------------------------

Annex 2 - Security measures

Area	Measure
Separation	Each customer has its own database and file store.
Encryption	TLS for all traffic; databases, files and backups encrypted at rest.
Access by users	Role, access-group and site-scope controls set by the customer; passkey and multi-factor sign-in available; password hashing with a modern algorithm; idle session time-out.
Access by our staff	Limited to staff who need it; multi-factor sign-in; access logged; "log in as" sessions recorded as the staff member, with the user they acted as.
Logging	Append-only audit trail of changes; security events recorded and reviewed.
Backups	Databases backed up at least daily, encrypted and held separately from the live system. File stores are backed up only where the Schedule of Services includes file backup.
Change control	Releases pass automated tests and security checks before they are deployed, and business software releases reach a demonstration instance before customers.
Testing	Security assessment of releases; independent third-party security audit and penetration testing (most recently by Vemo IT, July 2026).
People	Confidentiality agreements for staff and contractors; security and privacy training; access removed on leaving.
Incidents	Documented response plan; customer notice under clause 8.