Data Processing Agreement

Version 1.3

Standalone global data protection addendum
Teamgo Pty Limited ABN 54 164 380 161

Document status	Effective date	Use
Current version	14 September 2026	Incorporation into customer agreements or optional countersignature

How this addendum takes effect

This Data Processing Agreement, including its Schedules and the Transfer Terms incorporated under Schedule 4, forms part of the agreement under which Teamgo provides the Services to Customer. It becomes binding on the date the Agreement becomes effective, the date Customer accepts it by reference, or the date of the last signature below, whichever first applies to the parties' relationship.

A customer may execute the signature page for procurement or compliance purposes. Countersignature does not create a separate service term, price, liability regime or governing law unless the parties expressly agree otherwise in writing.

Data Processing Agreement

This Data Processing Agreement (DPA) is entered into between Teamgo Pty Limited ABN 54 164 380 161 (Teamgo) and the customer identified in the Agreement or signature block (Customer). It governs Teamgo's Processing of Customer Personal Data in providing the Services.

1 Definitions

1.1 Agreement means the SaaS agreement, order form, statement of work, online terms, reseller customer agreement or other contract under which Teamgo provides the Services to Customer.

1.2 Applicable Data Protection Law means any law binding on a party that regulates the Processing, privacy, security, breach notification or protection of Customer Personal Data under the Agreement. It includes, where applicable, the Australian Privacy Act 1988 (Cth) and Australian Privacy Principles, the EU GDPR, the UK GDPR, the UK Data Protection Act 2018 and applicable national laws implementing or supplementing them.

1.3 Customer Personal Data means Personal Data Processed by Teamgo on behalf of Customer in connection with the Services. It excludes data for which Teamgo determines the purposes and means of Processing, which Teamgo handles as an independent controller under its applicable privacy notice.

1.4 Data Protection Laws, Data Subject, Personal Data, Personal Data Breach, Process, Processing, Processor, Controller and Supervisory Authority have the meanings given in Applicable Data Protection Law. Where a law uses materially similar terms, those terms have the corresponding meaning.

1.5 EU GDPR means Regulation (EU) 2016/679. UK GDPR has the meaning given in section 3(10), as supplemented by section 205(4), of the UK Data Protection Act 2018.

1.6 Services means the Teamgo cloud software, applications, support and related services supplied under the Agreement.

1.7 Subprocessor means a third party engaged by Teamgo to Process Customer Personal Data on Customer's behalf in connection with the Services.

1.8 Transfer Terms means the transfer mechanism applicable under clause 11 and Schedule 4, including the EU SCCs, UK Addendum or UK IDTA, as applicable.

2 Scope and roles

2.1 This DPA applies only to Teamgo's Processing of Customer Personal Data on Customer's behalf. Customer is the Controller and Teamgo is the Processor. If Customer is itself a Processor, Customer appoints Teamgo as its subprocessor and represents that its instructions and appointment of Teamgo are authorised by the relevant Controller.

2.2 Each party remains responsible for its own Processing as an independent Controller. Teamgo may Process account, billing, relationship, security, service analytics and business contact data as an independent Controller to the extent it determines the purposes and means of that Processing. Teamgo will handle that data under Applicable Data Protection Law and its published privacy notice.

2.3 Schedule 1 describes the subject matter, nature, purpose and duration of the Processing, categories of Personal Data and categories of Data Subjects. The Agreement, Customer's documented configuration and use of the Services, and lawful written instructions accepted under clause 3 further specify the Processing.

3 Documented instructions

3.1 Teamgo will Process Customer Personal Data only on Customer's documented instructions, including to provide, secure, support and improve the Services as necessary to perform the Agreement, unless Applicable Data Protection Law requires otherwise. If law requires other Processing, Teamgo will inform Customer before Processing unless the law prohibits notice on important grounds of public interest.

3.2 Customer instructs Teamgo to Process Customer Personal Data as described in this DPA and the Agreement; in accordance with Customer's use and configuration of the Services; to prevent or address technical or security problems; and as otherwise documented and agreed by the parties.

3.3 Teamgo will promptly inform Customer if, in Teamgo's opinion, an instruction infringes Applicable Data Protection Law. Teamgo may suspend the affected Processing until Customer modifies or confirms the instruction. Teamgo is not required to provide legal advice or independently determine whether Customer's Processing is lawful.

3.4 Instructions outside the scope of the Agreement require Teamgo's prior written agreement and may be subject to reasonable fees, technical limitations and revised terms.

4 Customer responsibilities

4.1 Customer will comply with Applicable Data Protection Law and is responsible for its collection and use of Customer Personal Data, including providing required notices, establishing a lawful basis, responding to Data Subjects, and obtaining consents where required.

4.2 Customer will ensure its instructions are lawful and that it has the right to disclose Customer Personal Data to Teamgo. Customer will not use the Services to Process data prohibited by the Agreement or unsupported by the Services.

4.3 Customer will configure retention, access, authentication, integrations and privacy settings appropriately; keep credentials secure; restrict authorised users; and provide accurate instructions and contact details.

4.4 Customer acknowledges that visitor management workflows may collect sensitive or special category data if Customer configures them to do so. Customer must determine whether that collection is necessary and lawful and apply any additional safeguards required by law. Customer must not enable facial recognition or biometric processing unless the feature is available, the parties have confirmed the applicable provider and safeguards, and Customer has satisfied all legal requirements.

5 Personnel and confidentiality

5.1 Teamgo will ensure that persons authorised to Process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality and receive privacy and security training appropriate to their roles.

5.2 Teamgo will limit access to Customer Personal Data to personnel who require it to perform the Agreement and will apply role-based or otherwise appropriate access controls.

6 Security

6.1 Taking account of the state of the art, implementation costs, and the nature, scope, context and purposes of Processing, as well as risks to individuals, Teamgo will implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to it. Schedule 2 describes the measures currently intended for the Services.

6.2 Teamgo may update its measures to reflect technical and operational developments, provided the overall level of protection is not materially reduced during the applicable service term.

6.3 Customer is responsible for assessing whether the Services and Customer's configuration meet Customer's legal and security requirements. Customer will notify Teamgo promptly of any vulnerability or suspected compromise affecting the Services and will not perform intrusive security testing without prior written authorisation.

7 Personal Data Breaches

7.1 Teamgo will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data. Teamgo's notification is not an acknowledgement of fault or liability.

7.2 To the extent information is available, Teamgo will describe the nature of the breach, affected data and Data Subjects, likely consequences, measures taken or proposed, and a contact for follow-up. Teamgo may provide information in phases and will take reasonable steps to contain, investigate and mitigate the breach.

7.3 Customer is responsible for determining whether notice to a Supervisory Authority, Data Subject or other person is required and for issuing that notice. Teamgo will provide reasonable assistance taking account of the nature of Processing and information available to Teamgo.

8 Data Subject requests

8.1 Taking account of the nature of the Processing, Teamgo will provide appropriate technical and organisational assistance, insofar as possible, for Customer to fulfil requests to exercise Data Subject rights under Applicable Data Protection Law.

8.2 If Teamgo receives a request relating to Customer Personal Data, Teamgo will, unless prohibited by law, direct the requester to Customer or promptly forward the request. Teamgo will not respond substantively except on Customer's documented instruction or as required by law.

8.3 Customer should use available self-service export, correction, anonymisation, restriction and deletion functions before requesting additional assistance. Additional assistance may be subject to reasonable fees where permitted by law and disclosed in advance.

9 DPIAs consultations and regulatory assistance

9.1 Taking account of the nature of Processing and information available to Teamgo, Teamgo will provide reasonable assistance with Customer's data protection impact assessments, prior consultations and regulatory enquiries concerning Teamgo's Processing of Customer Personal Data.

9.2 Customer remains responsible for deciding whether a DPIA or consultation is required and for its content and submission. Teamgo may charge reasonable fees for bespoke assistance beyond information generally made available to customers, unless the need for assistance arises from Teamgo's breach of this DPA.

10 Subprocessors

10.1 Customer gives Teamgo general written authorisation to engage the Subprocessors listed at https://www.teamgo.co/terms/subprocessors/ and other Subprocessors appointed in accordance with this clause. Schedule 3 explains how the live list applies.

10.2 Teamgo will impose written data protection obligations on each Subprocessor that provide a level of protection for Customer Personal Data materially equivalent to the obligations applicable to Teamgo under

this DPA, as required by Applicable Data Protection Law. Teamgo remains responsible to Customer for the Subprocessor's performance of those obligations to the extent required by law and the Agreement.

10.3 Teamgo will give Customer advance notice of a new or replacement Subprocessor by updating the live list and through the notification method selected by Teamgo for subprocessor updates. Customer may object on reasonable data protection grounds by written notice within the notice period stated in Schedule 3.

10.4 The parties will work in good faith to address a valid objection. Teamgo may offer a commercially reasonable configuration change or alternative. If Teamgo cannot reasonably resolve the objection, either party may terminate only the affected Services on written notice. Customer's exclusive remedy is a pro-rata refund of prepaid fees for the terminated period, unless the Agreement provides another remedy.

10.5 A provider connected directly under Customer's own account or agreement may act as Customer's processor rather than Teamgo's Subprocessor. Customer is responsible for authorising and configuring those integrations. Teamgo remains responsible only for its own Processing and transfer of Customer Personal Data to the integration as instructed.

11 International transfers

11.1 Teamgo may Process Customer Personal Data in Australia and in other locations used to provide the Services, subject to the Agreement, Customer's selected hosting region, the live subprocessor list and Applicable Data Protection Law.

11.2 Each party will ensure that any Restricted Transfer it makes has a lawful transfer mechanism. If Customer transfers EEA Personal Data to Teamgo in a country not recognised as adequate, the EU SCCs apply as set out in Schedule 4. If Customer transfers UK Personal Data to Teamgo in a country not covered by UK adequacy regulations, the UK transfer mechanism selected in Schedule 4 applies.

11.3 Teamgo will provide information reasonably necessary for the parties to assess the transfer; implement supplementary measures where reasonably necessary; and notify Customer if Teamgo can no longer comply with the applicable Transfer Terms. The parties will cooperate in good faith on a documented transfer assessment.

11.4 If Teamgo receives a legally binding request from a public authority for Customer Personal Data, Teamgo will, to the extent legally permitted, notify Customer, review the request's legality, challenge unlawful or disproportionate requests where there are reasonable grounds, disclose only the minimum data legally required, and document its response as required by the applicable Transfer Terms.

11.5 If a conflict exists between this DPA and mandatory provisions of the applicable Transfer Terms, the Transfer Terms prevail for the Restricted Transfer.

12 Return and deletion

12.1 During the service term, Customer may use available functionality to export, anonymise or delete Customer Personal Data, subject to the Agreement and technical limitations.

12.2 On termination or expiry of the affected Services, and at Customer's choice where Applicable Data Protection Law requires, Teamgo will return or delete Customer Personal Data and delete existing copies, unless law requires retention. Data stored in backups may remain until overwritten or deleted under Teamgo's normal backup lifecycle, provided it remains protected and is not restored except for disaster recovery or legal compliance.

12.3 Teamgo may retain Customer Personal Data to the extent required by law, provided it isolates the data from further Processing except for the required purpose and deletes it when retention is no longer required.

13 Compliance information and audits

13.1 Teamgo will make available information reasonably necessary to demonstrate compliance with its obligations as Processor under Applicable Data Protection Law. Teamgo may satisfy requests by providing relevant policies, security summaries, certifications, independent audit reports, questionnaires or other evidence, subject to confidentiality and security restrictions.

13.2 If available evidence is not reasonably sufficient, Customer may request an audit no more than once in any 12-month period, except following a confirmed Personal Data Breach affecting Customer Personal Data or where a Supervisory Authority requires an audit. The audit must be conducted by an independent qualified auditor, during normal business hours, on reasonable advance notice, without accessing other customers' data or disrupting Teamgo's operations.

13.3 The parties will agree the audit scope, timing and safeguards in advance. Customer will bear its audit costs and reimburse Teamgo's reasonable costs, unless the audit identifies Teamgo's material breach of this DPA. Teamgo may object to an auditor that is a competitor, lacks appropriate qualifications, or will not accept reasonable confidentiality and security obligations.

13.4 Teamgo will cooperate with a competent Supervisory Authority as required by Applicable Data Protection Law.

14 Records and regulatory communications

14.1 Each party will maintain records required of it under Applicable Data Protection Law. Teamgo will provide Customer with information reasonably necessary for Customer's records concerning the Processing described in this DPA.

14.2 Each party will promptly inform the other of a regulatory communication specifically concerning the other party's Processing under this DPA, unless prohibited by law. No party may make submissions on behalf of the other without written authority.

15 Liability

15.1 The liability exclusions, limitations, procedures and remedies in the Agreement apply to this DPA and the Transfer Terms to the maximum extent permitted by law. Nothing in this DPA limits liability that cannot lawfully be limited or prejudices rights granted directly to Data Subjects under the Transfer Terms.

15.2 Any claims under this DPA and the Agreement are aggregated for purposes of applying liability caps and are not subject to separate or additional caps merely because they arise under this DPA.

16 Order of precedence

16.1 For Processing of Customer Personal Data, the order of precedence is: mandatory Transfer Terms; this DPA; an executed order form or negotiated data protection amendment; and the remainder of the Agreement. A later document prevails only if it expressly identifies the provision it changes.

16.2 This DPA does not amend commercial terms unrelated to Processing, including fees, service levels, intellectual property, warranties, indemnities or general liability, except where it expressly states otherwise.

17 Term and survival

17.1 This DPA begins when it takes effect under the introductory section and continues while Teamgo Processes Customer Personal Data on Customer's behalf.

17.2 Obligations that by their nature continue after termination, including confidentiality, deletion, audit cooperation for the relevant period and Transfer Terms, survive for as long as Teamgo retains Customer Personal Data.

18 Governing relationship and notices

18.1 The governing law and dispute resolution provisions of the Agreement govern this DPA, except where Applicable Data Protection Law or the Transfer Terms require otherwise.

18.2 Notices under this DPA must be sent under the Agreement's notice procedure. Privacy and security communications may also be sent to the contacts designated by each party. Customer must keep its administrative and privacy contacts current.

18.3 This DPA may be executed electronically and in counterparts. A person accepting or signing it represents that they have authority to bind the relevant party.

Schedule 1 Details of Processing

Field	Description
Subject matter	Processing Customer Personal Data to provide, host, operate, secure, maintain and support the Teamgo visitor management and related workplace services ordered by Customer.
Duration	For the service term and any limited period after termination during which Teamgo returns, deletes or lawfully retains Customer Personal Data.
Nature and purpose	Collection, recording, organisation, hosting, storage, retrieval, display, transmission, notification, integration, support, troubleshooting, security monitoring, backup, export, anonymisation and deletion as configured or instructed by Customer.
Frequency	Continuous or event-driven according to Customer's use of the Services.
Data subjects	Visitors and prospective visitors; Customer employees, contractors and authorised users; hosts and reception personnel; emergency contacts; event or meeting attendees; delivery personnel; and other individuals whose data Customer submits.
Personal Data	Identity and contact details; employer or organisation; visit details, date, time, location, host and purpose; photographs, signatures, acknowledgements, access or badge information; vehicle or delivery details; device, log, authentication and usage data; messages and notification details; questionnaire responses; and data entered in customer-configured fields.
Potential sensitive data	Health, accessibility, safety, vaccination or screening responses; government identifiers; children's data; and biometric data only if a separately approved feature is offered and lawfully enabled. Collection depends on Customer configuration and must be minimised.
Special processing	No automated decision-making with legal or similarly significant effects is intended as part of the standard Services. Optional integrations and customer-configured workflows may change the data flow.
Return and deletion	Customer-controlled export, anonymisation and deletion features where available; post-termination handling under clause 12 and confirmed operational retention periods.
Controller instructions	The Agreement, this DPA, order forms, documented product configuration, support requests from authorised contacts, and other written instructions accepted by Teamgo.

Schedule 2 Technical and Organisational Measures

Teamgo will maintain measures appropriate to the risk of the Processing. The measures below describe the safeguards applicable to the Services, subject to Customer's service plan, configuration and use.

Control area	Measure
Governance and risk	Documented privacy and information security responsibilities, risk assessment, policies, workforce training and periodic control review.
Access control	Unique accounts, least-privilege access, role-based controls where appropriate, access review, prompt removal of access and strong authentication for privileged or production access.
Authentication	Password and session controls appropriate to risk, multi-factor authentication for privileged access, and supported customer identity or SSO options where included in the service plan.
Encryption	Encryption of Customer Personal Data in transit using current secure protocols and at rest using platform or service encryption appropriate to the storage system. Keys and secrets are access-controlled and managed separately from application data where practicable.
Network and infrastructure	Segmentation or equivalent logical separation, hardened configurations, controlled administrative access, monitoring, patching and protections against common network threats.
Application security	Secure development practices, change control, code review and testing proportionate to risk, dependency and vulnerability management, and remediation prioritised by severity.
Tenant separation	Logical controls designed to prevent one customer from accessing another customer's data.
Logging and monitoring	Security-relevant logging, monitoring and alerting designed to detect unauthorised access, misuse and service anomalies, with access to logs restricted.
Incident management	Documented detection, escalation, containment, investigation, recovery and communication procedures, supported by assigned responsibilities and periodic review or exercises.
Availability and recovery	Backups, redundancy and recovery procedures appropriate to the Services, with restoration testing and protected backup access.
Data lifecycle	Tools or procedures for retention, export, anonymisation and deletion; disposal of media and records using methods appropriate to sensitivity; restrictions on restoration of deleted data from backup.
Personnel and suppliers	Confidentiality obligations, role-appropriate training, proportionate personnel controls, supplier due diligence and written data protection and security obligations.
Physical security	Physical and environmental safeguards provided by Teamgo and its hosting providers for facilities that host systems or from which authorised access occurs.
Testing and assurance	Periodic assessment of safeguards, vulnerability management and independent testing or assurance where adopted by Teamgo. Findings are tracked and remediated according to risk.
Customer controls	Administrative roles, permissions, retention and privacy settings, deletion or anonymisation tools, exports and supported identity integrations, subject to plan and configuration.

Schedule 3 Subprocessors

3.1 Operative list

The current and operative list of Subprocessors is maintained at https://www.teamgo.co/terms/subprocessors/ and is incorporated into this DPA by reference. Customer should consult that page for current provider names, purposes, locations and feature dependencies. Teamgo will maintain an update process consistent with clause 10.

3.2 Notice and objection process

Item	Position
Advance notice	At least 30 days before a new Subprocessor begins Processing, except an urgent replacement required for security, continuity or law, where notice will be given as soon as reasonably practicable.
Notification method	Email to Customer's administrator or designated privacy contact and an update to the live Subprocessor List.
Objection period	Customer must object within the advance notice period and identify specific, reasonable data protection grounds.
Resolution	Good-faith mitigation, alternative configuration if commercially reasonable, or termination of affected Services under clause 10.4.

Schedule 4 International Transfers and SCC Information

4.1 Restricted Transfers

This Schedule applies when Customer Personal Data is transferred to Teamgo or a Subprocessor in a country for which the relevant EEA or UK transfer law requires an approved safeguard. It does not create a Restricted Transfer where none otherwise exists.

4.2 EU Standard Contractual Clauses

The standard contractual clauses adopted by European Commission Implementing Decision (EU) 2021/914 dated 4 June 2021 (EU SCCs) are incorporated by reference and completed as follows when they apply:

SCC item	Selection or information
Module	Module Two Controller to Processor where Customer is a Controller; Module Three Processor to Processor where Customer is a Processor.
Clause 9 subprocessors	Option 2 general written authorisation. The time period is the approved notice period in Schedule 3.
Clause 11 redress	The optional independent dispute-resolution language does not apply.
Clause 13 supervision	The competent authority determined under clause 13 of the EU SCCs based on the exporter's establishment, representative or affected Data Subjects.
Clause 17 governing law	Option 1 applies. The EU SCCs are governed by the law of Ireland.
Clause 18 courts	The courts of Ireland, without limiting a Data Subject's rights under clause 18(c) of the EU SCCs.

SCC item	Selection or information
Annex I parties	Exporter: Customer and relevant affiliates described in the Agreement or signature page. Importer: Teamgo Pty Limited ABN 54 164 380 161, Australia. Contacts must be completed from the Agreement or signature page.
Annex I transfer	The Processing described in Schedule 1; transfers may occur continuously for the service term; sensitive data only as customer-configured and subject to the safeguards in this DPA.
Annex II security	The verified measures in Schedule 2.
Annex III subprocessors	The operative list in Schedule 3 and the process in clause 10.

For the EU SCCs, this DPA and Agreement provide additional commercial clauses only to the extent they do not contradict the SCCs or prejudice Data Subject rights. Signatures to this DPA are deemed signatures to the applicable EU SCC module.

4.3 UK transfers

For a transfer governed by the UK GDPR, the parties will use the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 (UK Addendum), unless the parties select the UK International Data Transfer Agreement (UK IDTA) in writing.

UK Addendum item	Completion
Table 1 parties	The parties and contacts identified in the Agreement, signature page and section 4.2 above.
Table 2 SCC version and modules	The EU SCCs and applicable Module Two or Module Three selections in section 4.2.
Table 3 appendix information	Schedules 1, 2 and 3 of this DPA.
Table 4 termination	Both the Importer and the Exporter may end the UK Addendum in accordance with section 19 if the ICO issues a revised Approved Addendum.
Alternative mechanism	The UK IDTA applies only if expressly selected in an order form or signed amendment and completed with equivalent processing and security information.

4.4 Switzerland and other jurisdictions

Where Swiss data protection law applies and permits use of the EU SCCs, references in the EU SCCs will be adapted as necessary to include Switzerland, the Swiss Federal Act on Data Protection and the competent Swiss authority, while preserving the SCCs' substantive protections. For another jurisdiction, the parties will execute or incorporate a valid local transfer mechanism where required.

4.5 Transfer assessment information

Topic	Information and action
Importer country	Australia, plus Subprocessor countries shown on the live list and relevant provider documentation.
Importer role	Processor or subprocessor as specified by the applicable module.

Topic	Information and action
Data and safeguards	Schedules 1 and 2, Customer's hosting-region selection, encryption and access restrictions, and Subprocessor contractual safeguards.
Government access assessment	The parties will assess relevant Australian law and each material onward-transfer country using reasonably available information and will document any supplementary measures required by Applicable Data Protection Law.
Review trigger	Material change to the transfer, law, government access practices, hosting region, Subprocessor chain or supplementary safeguards.

Execution

The parties may sign this DPA to record their agreement. If the DPA is incorporated into an Agreement and accepted through that Agreement, signatures below are optional.

For Teamgo Pty Limited	For Customer
Signature: _____ Name: _____ Title: _____ Date: _____	Legal name: _____ Signature: _____ Name: _____ Title: _____ Date: _____

Customer and transfer details

Field	Details
Customer legal name	
Registered address	
Privacy contact name and email	
Agreement or order reference	
Customer role	Controller / Processor / Both, depending on processing
Applicable hosting region	
EU representative if applicable	
UK representative if applicable	
Competent supervisory authority	
Special processing instructions	