ProcureLabs Enterprise Terms

Enterprise order form

ProcureLabs Pte. Ltd. | Enterprise Terms v1.0 | Effective Date as stated in the Order

This Order, the incorporated Bonterms Cloud Terms and Data Protection Addendum, the Additional Terms and Schedules A–D form the Agreement between Provider and Customer. The Order and completed processing details identify the purchased service and Customer's instructions.

Order field	Agreed entry
Provider	ProcureLabs Pte. Ltd. (UEN 202606070W), 160 Robinson Road #14-04, Singapore Business Federation Centre, Singapore 068914. Notices: admin@procure-labs.com.
Customer	[exact legal name, registration number, registered address and authorised contracting entity.]
Order and effective date	[order number, execution date, service start date.] No date is backdated.
Governing law and Courts	[Governing Law: country or jurisdiction.] [Courts: agreed courts and venue.] Cloud Terms §22.2 applies.
Service and users	ProcureLabs procurement SaaS. [purchased modules, user/affiliate scope, usage limits, permitted data, integrations and implementation deliverables.]
Term and renewal	[initial term and renewal election.] No automatic renewal unless this Order expressly specifies renewal length and notice period.
Fees and payment	[currency, subscription fees, usage charges and any cap, taxes, invoice schedule.] Payment within 30 days of invoice. No unquoted professional services or expenses.
Contacts	[commercial, support, privacy and security notice contacts and approved customer administrators.]
Service commitments	Schedule B applies. commercially reasonable availability efforts, without a numeric uptime guarantee, service credits, 24/7 support or a full-service RPO/RTO. Any enhanced commitment must be written here.
AI and locations	Schedule C applies only to the functions and data the Customer selects in the activation record. Primary AI configuration: EU Azure OpenAI and EU Bedrock. Singapore core hosting remains separate.
Incorporated documents	Bonterms Cloud Terms v1.0; Additional Terms AT1–AT10 below; Bonterms DPA v2.0 Attachment Version and completed DPA Details; Schedules A–D; the versioned AUP in Schedule B. AI Addendum v2.0 is NOT incorporated.

Acceptance wording: The parties agree to this Order and the exact incorporated versions supplied with it, including the completed DPA Details and agreed activation record. A link to a later web version does not change this Agreement. Only the parties' authorised representatives may agree changes in writing.

For Provider: [name and role] Signature: [signature] Date: [date].

For Customer: [name and role] Signature: [signature] Date: [date].

Additional terms and contract hierarchy

These Additional Terms modify the identified provisions of the incorporated standard forms. All other provisions remain unchanged.

AT1 Scope and order of precedence

For Cloud Terms §22.5, this signed Order's expressly identified Additional Terms prevail over the Schedules and Cloud Terms. Commercial entries such as fees and scope control only their subject matter. Within data protection matters, mandatory transfer clauses and DPA Exhibit B take priority as provided in DPA §2.6; DPA Additional Terms, then the DPA, control over conflicting commercial provisions. An Order cannot override mandatory law or mandatory transfer-clause protections. A later Order changes an earlier agreement only where it names the provisions and scope being changed.

AT2 Agreement versions and operational updates

For Cloud Terms §§22.6–22.7, contract amendments require a writing signed, including valid electronic signatures, by both authorised representatives. Notified operational updates may improve the service or reflect changing practices but may not retroactively apply or materially reduce the overall agreed support, SLA or security obligations during the Subscription Term. A new recipient, processing purpose, country or retention expansion follows the DPA and Schedule C approval process; posting a revised web page is not customer consent. Existing agreements with other customers are unaffected.

AT3 Availability and support

Cloud Terms §7.2 is replaced by: Provider will use commercially reasonable efforts to maintain availability of the purchased Cloud Service. Schedule B specifies the standard support arrangements. No numeric uptime commitment or service-credit scheme applies unless an executed Order expressly identifies the commitment, measurement method, exclusions and remedy. The standard 99.9% fallback in Cloud Terms §7.2 does not apply. Planned maintenance and supplier failures are not automatically excluded from an expressly agreed SLA; the applicable Order determines the treatment.

AT4 Data use and AI training

Cloud Terms §5.4 is supplemented: Usage Data excludes Customer Data, including identifiable prompts, outputs, uploaded content and customer-confidential procurement information. No right to use Customer Data for shared model training, fine-tuning, resale, advertising or another customer's benefit is granted. Provider will not opt Customer Data into a model provider's training or product improvement. Any separately requested reuse requires a separate written agreement and lawful basis. Aggregation or de-identification is not itself permission to reuse Customer Data. Necessary security and abuse monitoring remains subject to Schedule D and the applicable DPA.

Additional terms for data and AI

AT5 Data types and testing

Cloud Terms §9.2(b) and the Sensitive Data definition in §23 are modified only as follows. Ordinary procurement records, including supplier contacts, employee business names/emails, roles, spend, invoices, contracts and purchase orders, are permitted within the purchased scope. Necessary business bank-account and payment-routing numbers are permitted only for a feature expressly identified in the completed DPA Details, with the precise fields, purpose, access restrictions and handling safeguards recorded. Such fields must be excluded or masked before AI processing unless the specific AI use and safeguards are separately agreed in writing. All other financial-account numbers, payment-card numbers and security codes, individual government identifiers, health records and other Sensitive Data remain excluded from the standard offer. Any exception requires a separate written scope and safeguards before processing. Passwords, API keys and recovery codes must never be submitted as procurement records, attachments or AI prompts; legitimate integration credentials may be entered only through an approved secure credential-entry flow. Customer must have the rights required by §9.1; Provider remains responsible for its obligations for permitted data. Redaction or automated screening is not a guarantee of anonymisation or safety. Written, scoped security testing agreed with Provider is permitted notwithstanding §9.3(d); unapproved disruption or access remains prohibited.

AT6 Approved processing and transfers

The paragraph in DPA §10.1 permitting necessary global processing is replaced by: Provider may process Customer Personal Data only for the functions, recipients and processing locations set out in the completed DPA Details, Schedule C and agreed activation record, or as required by applicable law subject to the DPA's notice duties. This includes identified supplier support, security and operational processing. No general permission for unrestricted global processing is given. New subprocessors require at least 30 days' advance notice and the DPA objection process. Material expansion beyond the agreed processing scope, including a new purpose or unapproved location, requires documented Customer agreement before activation. Routine changes within the agreed purpose, data, hosted service and location scope do not require a new contract. EU inference and Singapore hosting are separate facts; neither is a promise that all ancillary processing stays in that location.

DPA §§1.10 and 3.3 are clarified: each party complies with the data protection laws applicable to its role and processing, including the Singapore PDPA, Australian Privacy Act 1988 and New Zealand Privacy Act 2020 where applicable. "Processor" includes "data intermediary" for the relevant Singapore processing. EU/UK/Swiss and US terms apply only to the extent triggered. Additional comparable-protection and transfer safeguards must be completed where required; an inference region or hosting label is not a transfer mechanism.

AT7 Return deletion and records

Cloud Terms §14.4 and DPA §8 are supplemented by Schedule D. Provider will make Customer Data reasonably available for export for 30 days after termination, subject to security restrictions and lawful suspension, unless Customer directs earlier deletion. Provider will begin the instructed return/deletion process promptly and complete active-system deletion within 60 days after termination without requiring a further request, subject to specifically documented legal obligations or holds and the agreed residual-copy schedule. Provider will address earlier lawful deletion instructions promptly and meet applicable mandatory duties. No routine retention policy creates an unrestricted exception. Retained copies remain protected, access-restricted and unused for ordinary service or training; if restored, applicable deletion instructions must be reapplied. A deletion certificate states actual scope, date, method and outstanding exceptions. It must not certify physical deletion or complete supplier expiry without supporting evidence.

AT8 Incident notices and individual requests

The DPA Specified Notice Period is 48 elapsed hours, including weekends and public holidays: Provider will notify Customer without undue delay, and no later than 48 hours after becoming aware of a Security Incident, with available information, identified uncertainties and subsequent updates. Initial notice is not delayed until the investigation is complete. Provider promptly refers direct individual requests concerning Customer-controlled records to Customer and assists; Provider does not independently disclose, correct or delete such records except on Customer instructions or where legally required. Provider remains responsible for requests concerning data it controls independently. This obligation operates outside standard support hours. Notice is not an admission of fault. Non-compromising unsuccessful attempts do not by themselves constitute a Security Incident under the DPA.

Additional terms for AI and liability

AT9 AI services and responsibility

The AI functions selected in the agreed scope are provided through the hosted services identified in Schedule C. Azure-hosted decision support is included within the Azure service description. Provider remains responsible for its contracted service and subcontracted service performance under this Agreement. Human review does not remove Provider's security, privacy or service obligations. AI outputs require appropriate human verification; no permission for autonomous spending, payment, signature or external commitment is granted by this Agreement. No zero-retention warranty or new AI-output indemnity is added. The agreed function and processing record controls which AI services may be enabled. AI outputs may contain errors, omissions or bias and are not legal, financial or audit advice. Customer must independently verify material outputs before use. This limitation does not remove the service warranties or Provider obligations expressly stated elsewhere in the Agreement.

AT10 Liability definitions

Cloud Terms §16.5 is replaced with the following definitions. Sections 16.1–16.4 otherwise remain unchanged, including §16.3's treatment of the consequential-damages waiver for Enhanced Claims and Uncapped Claims.

"General Cap" means the amounts paid or payable by Customer to Provider under this Agreement in the 12 months immediately preceding the first incident giving rise to liability.

"Enhanced Cap" means three times the General Cap.

"Enhanced Claims" means (a) Provider's breach of §5.2 (Security), (b) either party's breach of §5.3 (DPA), (c) the indemnifying party's obligations under §17 to the extent they concern a third-party claim of intellectual-property infringement or misappropriation, and (d) either party's breach of §18 (Confidentiality).

"Uncapped Claims" means only liabilities that cannot be limited by applicable Law. Liability is uncapped only to the extent that Law prohibits the relevant limitation.

For clarity, a direct intellectual-property claim or a non-IP indemnity obligation that is not an Enhanced Claim or Uncapped Claim falls within the General Cap. An overlapping claim is classified by the obligation actually breached; labelling the same loss under more than one cause of action does not create multiple recoveries.

No additional AI-output copyright indemnity is created by these Additional Terms. Existing §17 obligations continue subject to their terms and these liability definitions.

DPA details for each enterprise customer

These details complete and expressly incorporate Bonterms DPA v2.0 Attachment Version into the signed enterprise Order. DPA Additional Terms are AT1, AT2 and AT4–AT10, with Schedules A, C and D. Customer-specific choices below must be completed before signature.

Processing detail	Agreed scope
Main Agreement and DPA date	The enterprise Order [number and date] incorporating Cloud Terms v1.0 and this package version. Effective on the agreed Order effective date.
Customer and role	[entity, address, privacy contact and business activities; select Controller or Processor and identify the relevant upstream authority if Customer is a Processor.]
Provider and role	ProcureLabs Pte. Ltd.; address on the Order; privacy contact admin@procure-labs.com. Processor/data intermediary for Customer Personal Data. Service: procurement SaaS analytics, workflow, document management and authorised AI assistance.
People whose data is involved	Authorised users and personnel; supplier/vendor representatives; procurement, finance and approver contacts; contract counterparties and signatories where the relevant feature is authorised. [remove unused categories and identify any other category.] Job applicants, patients and consumers are not default scope.
Data categories	Business names/contact details, job roles, account and tenant identifiers, authorised access/audit metadata; supplier, spend, invoice, purchase-order and contract records; communications, uploaded files and authorised AI inputs/outputs. Personal information may occur within business documents. [actual fields, datasets, affected jurisdictions and volume/risk category.]
Restricted data	No payment-card data, individual government identifiers, health or other Sensitive Data by default. No procurement uploads or AI prompts containing secrets. [confirm none, or identify the necessary business bank/routing fields, feature, access restrictions and AI-exclusion/masking safeguards under AT5; separately agree any specific AI use.] Secure integration credential-entry flows are separate from procurement content.
Nature and purpose	Collection, import, storage, retrieval, analysis, extraction, indexing, authorised inference, display, collaboration, export, restriction and instructed deletion solely to provide the purchased services and follow documented instructions. No training or secondary reuse permission.
Frequency and duration	Continuous/on-demand while the selected service operates; Schedule D governs termination and residual copies. AI transfer occurs only for the enabled function and agreed data.
Recipients and locations	Versioned Schedule C plus the signed activation record. Optional services require their stated selection; a supplier appearing on a public catalogue is not blanket authorisation.
EU SCC details if applicable	[applicability/module, exporter details, designated EU Member State law and courts, competent supervisory authority under SCC Clause 13 and transfer assessment.] Use N/A only after applicability is checked. Complete the UK/Swiss adaptations where triggered.
Security and assistance	Schedule A. Subprocessor notice to the Customer privacy/security contacts by email at least 30 days before new processing, with the DPA objection process. Incident notice: AT8. Audit and rights assistance: DPA §§7 and 9.

The completed processing details and activation record constitute Customer’s instructions for the selected functions. Unselected functions and incomplete entries are not authorised by signing this Order. No retrospective authorisation of earlier processing is granted.

Schedule A Security measures

Provider will maintain the following measures for the purchased hosted service. Customer-specific configurations and enhanced services apply only where included in the Order.

Hosting encryption and access

The core application and primary managed database are hosted in Singapore. Customer records held in the managed database and object-storage services use cloud-provider encryption at rest; external application connections use TLS. Key custody and any customer-managed-key feature follow the purchased configuration. No statement here promises field-level encryption of every datum, end-to-end encryption or that Provider has no decryption access.

The application supports multi-factor authentication, role-based permissions and tenant access restrictions. Customer is responsible for its authorised users, appropriate roles and any customer-controlled identity-provider policy. Privileged background and administrative processing must enforce tenant scope in addition to database row-level security. Cloud supplier controls do not replace Provider’s application and administrative controls.

Development operations and incident handling

Provider maintains documented security and incident procedures, controls production changes through reviewed merge requests and required checks, and uses secret and dependency scanning. Production releases follow the controlled release process. Audit information is recorded for supported actions; coverage and retention depend on the feature. This is not a representation that every read, every privileged action or all telemetry is a complete, immutable audit trail.

Provider restricts access to personnel who need it for authorised work, maintains applicable confidentiality duties, and investigates reported vulnerabilities and incidents. Security reports may be sent to support@procure-labs.com. Customer incident notices follow AT8; an in-product announcement is not a substitute for a required individual contractual notice.

Backup recovery and supplier responsibilities

The managed database is configured for point-in-time recovery with a seven-day history. Database backups exclude uploaded object-file bytes. Object-file backup arrangements, if purchased, are identified separately in the Order and processing details. Recovery-time and recovery-point commitments apply only where expressly stated in the Order.

Provider maintains a supplier inventory and reviews service-specific data, access, transfer and retention conditions. Optional integrations and enhanced backup services are enabled only within the agreed scope. Any supplier certification applies to its stated scope. A ProcureLabs certification or independent assurance report forms part of the service commitments only where expressly identified in the Order.

Evidence and changes

On reasonable request and subject to confidentiality and third-party restrictions, Provider will supply relevant available security information and support the DPA audit process. Certificates and reports are identified by issuer, scope and date. Operational changes follow AT2.

Schedule B Support availability and acceptable use

Standard support

Support channel: support@procure-labs.com. Standard staffed hours are Monday–Friday, 09:00–18:00 Singapore time, excluding Singapore public holidays. Requests may be emailed at any time. During staffed hours, Provider aims to give an initial response within four business hours for a service-wide outage or suspected data-loss incident and one business day for other faults. These are response targets, not resolution guarantees. Dedicated engineers, 24/7 staffing and shorter response commitments require an expressly agreed Order. The incident-notice deadline in AT8 is separate and runs in elapsed hours outside these support hours.

Availability measurement and maintenance

AT3 applies: no numeric uptime guarantee or credits form part of the standard offer. If the parties agree a numeric SLA, the Order must define affected service functions, observation interval, denominator, incident start/end evidence, partial degradation, exclusions and remedies. Provider will give advance email notice of planned maintenance where reasonably practicable. No blanket third-party-failure exclusion is added. Urgent security or reliability work may require shorter notice with explanation and incident records.

The standard offer does not promise monthly uptime reports by a fixed date, a public status page, cross-region failover or a 15-minute/one-hour whole-service RPO/RTO. Any later commitment must be measured, resourced and included in the Order; supplier backup features do not establish an end-to-end recovery result.

Versioned acceptable use rules

- Use the service for lawful enterprise procurement work within the purchased modules, data categories and usage limits. Keep credentials secure and promptly report suspected compromise.
- Do not upload malware, bypass controls, access another tenant’s information, disrupt the service, or conduct security testing without a written scope. Provider will consider reasonable coordinated security testing.
- Do not submit prohibited sensitive information. Necessary business bank/routing fields require the express AT5 record and must be excluded or masked before AI processing unless specifically approved. Never include passwords, API keys or recovery codes in procurement content or AI prompts; use only approved secure credential-entry flows. Automated screening is not a safety guarantee.
- Do not use the service for unlawful discrimination or solely automated decisions with legal or similarly significant effects on individuals without a separately approved lawful design and safeguards. Do not treat AI outputs as legal, audit or financial advice.
- Use only authorised integrations. Do not resell access, extract models, send spam or use Customer Data or outputs to violate another person’s rights. Any restriction on competing-model training follows the applicable agreed AI terms; no new supplier agreement is accepted by this AUP.

Enforcement follows the Cloud Terms’ suspension, cure and termination rules. Immediate proportionate protection may be necessary for a serious security risk or legal requirement; Provider will notify Customer and work to restore lawful use. A later web AUP version does not silently amend this signed version.

Schedule C Core processing and primary AI routes

The completed activation record identifies the services selected by Customer, the recipient legal entities, permitted data, processing locations and applicable transfer safeguards. Only those selected entries are authorised.

Function and recipient	Data and purpose	Processing locations and boundaries
Core hosting — Amazon Web Services	Application traffic, service metadata and hosted application processing.	Core application: Singapore, ap-southeast-1. Recipient legal entity and any ancillary edge, support or security locations: [Processing Details]. No unrestricted global-processing permission is granted.
Database Auth and Storage — Supabase	Customer records, account/authentication metadata, uploaded objects and database recovery data.	Database, Auth, Storage and database recovery: selected Singapore project region. Ancillary global support/operations, EU log centres and any configured CDN delivery are separately identified in the completed Processing Details, together with recipient entities and safeguards.
GPT and embeddings — Microsoft Azure OpenAI	Authorised chat/context, generated responses, text embeddings and decision support for the selected functions.	Sweden Central Azure resource with regional/EU Data Zone inference as identified in the activation record. Standard abuse monitoring applies unless a different approved arrangement is expressly recorded. Ancillary support/security processing and retention are specified in the Processing Details.
Claude inference — AWS Bedrock	Only authorised chat, document/context and extraction payloads for the agreed functions.	EU geographic inference profiles entered through Ireland may execute across the EU regions in the selected profile. The activation record specifies the model/API, retention mode, invocation logging and safety/legal exceptions. No general zero-retention commitment applies.

Azure-hosted OpenAI models are provided through Microsoft Azure; Claude models hosted by Bedrock are provided through AWS Bedrock. Direct OpenAI, Anthropic and Gemini API processing is outside this service configuration unless a separate purpose, recipient, location and authority are expressly agreed.

The completed Processing Details identify each relevant exporter/importer role, transfer instrument, onward recipient, access safeguard and supplementary measure. Applicable mandatory EU/UK/Swiss transfer clauses prevail. Singapore, Australian and New Zealand protections apply to the extent required for the relevant party, role and processing.

Schedule C Supporting services and activation record

Supporting service	Data and purpose	Agreed scope and locations
Resend	Recipient addresses and authorised transactional email content.	United States service inventory. Exact recipient entity, contracted region, onward recipients and retention: [Processing Details].
Inngest	Workflow identifiers, event/job metadata and any necessary bounded payload.	United States service inventory. Customer payloads are limited to the agreed workflow schema. Recipient entity, region and retention: [Processing Details].
Sentry	Error/performance metadata and any permitted diagnostic fields.	United States service inventory. Diagnostic fields and scrubbing controls are specified in the Processing Details, with the recipient entity, region and retention.
Upstash or other configured cache	Cache, rate-limit or session-related metadata within the configured scope.	Only if selected in the activation record. Recipient entity, configured region, payload categories and expiry: [Processing Details].
Microsoft 365 and SharePoint	Authorised business correspondence, support/legal records and selected company documents.	Correspondence and documents only within the agreed support or administration purpose. Recipient entities, locations, access and retention are separately recorded. Independent-controller company administration remains subject to the applicable privacy notice.
Stripe	Subscription/billing contacts, tokens and transaction metadata.	Payment-service roles and terms govern relevant independent-controller processing. Procurement documents must not be submitted to Stripe.
Optional electronic signing	Signer/contact details, documents and signature/audit records.	Excluded unless expressly selected. A selected service requires an agreed recipient, document scope, locations, retention and integration record.

Activation record to complete for each selected function

[function and permitted purpose; exact data categories and prohibited fields; recipient legal entity and approved onward recipients; company account/project and endpoint/deployment identity reference without keys; processing/storage/support/security locations; retention and exceptions; training/logging/cache settings; evidence references and review dates; Customer instructions and lawful basis/transfer instrument; required named Customer approvers and Provider reviewer; start date; withdrawal/disable route; verification result.]

Only the completed selected entries constitute the instructed service scope. Before an entry goes live, Provider verifies the relevant implementation and a bounded test against that entry; Customer supplies any approvals required by its agreed governance. A signature on an incomplete record is not approval of missing entries. New subprocessors follow the DPA’s 30-day notice/objection process, with express approval where the agreed record requires it.

Schedule D Retention return and deletion

The following retention rules apply by data category. The completed Processing Details specify any required provider-copy, security-log and external-copy periods. Retained copies remain protected and access-restricted, and may not be used for ordinary service or model training after the applicable deletion instruction.

Category	Retention and deletion rule
Customer records and uploads	During the service term as instructed. A 30-day export opportunity follows termination unless earlier deletion is requested. Active-system deletion is completed within 60 days after termination under AT7 without another request. Earlier lawful instructions are addressed promptly.
Chat output and embeddings	Follow the applicable Customer-record category and instructions. Deletion includes associated indexes, derived content and service copies within the agreed scope.
Security and audit records	Retain only for the documented necessary purpose, lawful basis and agreed period. Period, start point and deletion method: [Processing Details]. Separate content from operational metadata where practicable.
Database recovery copies	Seven-day configured PITR history. Access is restricted to recovery. Current restrictions and deletion instructions are reapplied after restoration. Object-file bytes are not included in database PITR.
Object backups and exports	Only destinations and copies expressly selected in the Order or activation record. Retention cycle and deletion method: [Processing Details]. No additional backup service is included by default.
Azure provider copies	Standard abuse-monitoring and selected service-state arrangements apply. The activation record identifies the endpoint/model, applicable periods, cache or stored-response features and safety/legal exceptions. No zero-retention warranty applies.
Bedrock provider copies	The activation record identifies the model/API, regional retention mode, invocation-logging configuration, periods and safety/legal exceptions. No zero-retention warranty applies.
Legal holds and company records	Only the records necessary for the specific obligation or hold are retained, with documented rationale, responsible person, review date and release condition. Independently controlled billing/legal records are governed by their applicable purpose and lawful basis.

The parties complete the periods and conditions relevant to the selected service in the Processing Details. Any required limit that cannot be met must be addressed by excluding the affected flow or expressly agreeing an alternative. Deletion certificates requested by Customer identify the actual scope, dates, residual copies and justified exceptions.

Incorporated forms and attribution

Bonterms Cloud Terms v1.0 © 2022 Bonterms and Bonterms DPA v2.0 Attachment Version © 2026 Bonterms, Inc. are incorporated as identified in the Order, subject to these Additional Terms and Schedules. The standard forms are licensed under Creative Commons Attribution 4.0 International. ProcureLabs modifications are stated separately. Use of the forms does not imply endorsement by Bonterms.

Cloud Terms: https://bonterms.com/standard/bonterms-cloud-terms-v1

DPA: https://bonterms.com/standard/dpa-v2-attachment-version

License: https://creativecommons.org/licenses/by/4.0/

Bonterms AI Addendum v2.0 is not incorporated. The AI terms in this Agreement are AT4, AT5 and AT9 together with the applicable processing and retention schedules.