DATA & PRIVACY

Data Processing Terms

Last updated: January 1, 2026 · v1.5

Document Details

Provider: Develab Pte. Ltd., 10 Anson Road #10-11 International Plaza, Singapore (079903), UEN Ref. 202402923E

Products: Rideum Suite — Bleustay, Bleudine and Bleudash

Version: 1.5 · Effective 01 January 2026

Contract role. These Terms are intended for Develab's processing of Customer Personal Data as a processor or data intermediary in providing the hosted Rideum Suite. They do not govern processing for which Develab independently determines the purposes and means; that processing is addressed in Develab's Privacy Policy.

These Data Processing Terms ("Terms" or "DPT") form part of the agreement between Develab Pte. Ltd. ("Develab", "Provider" or "Processor") and the customer identified in an Order ("Customer" or "Controller") for the Rideum Suite. They apply when Develab processes Customer Personal Data on Customer's behalf in connection with Bleustay, Bleudine, Bleudash or related subscribed services. Capitalised terms not defined here have the meanings in the End-User Licence and Subscription Agreement ("EULA").

1. Definitions and scope

1.1 Applicable Data Protection Law means privacy, data-protection and data-security law applicable to the relevant processing, including, where applicable, Singapore's Personal Data Protection Act 2012, Indonesia's Law No. 27 of 2022 on Personal Data Protection and its effective implementing rules, the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and other mandatory local requirements.

1.2 Key terms. "Controller" includes a personal data controller; "Customer Personal Data" means Personal Data contained in Customer Data that Develab processes on Customer's behalf; "Data Subject" means the identified or identifiable person to whom Personal Data relates; "Personal Data" includes personal data and personal information protected by Applicable Data Protection Law; "Personal Data Breach" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data; "Process" and "Processing" have their statutory meanings; "Processor" includes a personal data processor or data intermediary; and "Subprocessor" means a third party engaged by Develab to process Customer Personal Data on Customer's behalf.

1.3 Application. These Terms apply only to Customer Personal Data described in Schedule 1. Each party remains responsible for its own processing outside that scope. If Customer is itself a processor, references to Controller include Customer's relevant controller, and Customer warrants that it is authorised to appoint Develab as a subprocessor and issue the instructions in the Agreement.

1.4 Reseller transactions. Where Customer buys through an authorised reseller, Customer remains the Controller unless the applicable Order expressly identifies another role. A reseller may transmit Customer's documented instructions or provide support only to the extent authorised by Customer and Develab. The reseller may not amend these Terms, access Customer Personal Data or appoint Develab for unrelated processing without written authority.

1.5 Order of precedence. For Personal Data matters, these Terms prevail over the EULA, AUP and Order to the extent of conflict. A valid transfer mechanism in Schedule 4 prevails for restricted international transfers. All other commercial terms, including fees, liability and dispute terms, remain governed by the EULA or Order.

2. Roles and Customer instructions

2.1 Party roles. Customer determines the purposes and essential means of processing Customer Personal Data and acts as Controller. Develab acts as Processor when it processes that data solely to provide, secure, support and maintain the Services on Customer's documented instructions. The parties acknowledge that statutory terminology may differ by jurisdiction but intend to allocate responsibilities consistently with these roles.

2.2 Documented instructions. The Agreement, Customer's authorised configuration and use of the Services, support requests, and written instructions accepted by Develab constitute documented instructions. Develab will process Customer Personal Data only on those instructions, including for transfers, unless law requires otherwise. Where legally permitted, Develab will inform Customer before required processing.

2.3 Unlawful instructions. Develab will promptly inform Customer if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law. Develab may suspend the affected processing until Customer modifies or confirms the instruction. Develab is not required to provide legal advice or follow an instruction that would expose it or the Services to material legal, security or operational risk.

2.4 Independent-controller activities. Develab may act as an independent Controller for its own business-contact records, contracting, billing, fraud prevention, service security, legal compliance and aggregated or irreversibly de-identified analytics, to the extent permitted by law. Develab will describe such processing in its Privacy Policy and will not use Customer Personal Data for independent advertising or sell it as personal data.

3. Customer obligations

3.1 Lawfulness and transparency. Customer is responsible for the lawfulness, fairness and transparency of its processing; determining a valid legal basis; issuing required privacy notices; obtaining consents where needed; honouring Data Subject rights; and ensuring its instructions comply with Applicable Data Protection Law.

3.2 Data authority and minimisation. Customer warrants that it has the rights and authority to provide Customer Personal Data to Develab and instruct its processing. Customer will submit only data that is adequate, relevant and limited to what is necessary for authorised hospitality operations, and will not use free-text or support fields to store prohibited or unnecessary sensitive data.

3.3 Configuration and users. Customer is responsible for permissions, retention settings, exports, integrations, user accounts and administrator actions; for securely configuring the Services; and for ensuring Authorised Users and resellers comply with the Agreement. Customer will promptly revoke unnecessary access and notify Develab of suspected compromise.

3.4 Special data and minors. Unless expressly supported and stated in an Order, Customer will not use the Services to process payment-card authentication data, government identifiers, biometrics, health information, criminal records or other highly sensitive data. Guest records may include information about children or minors; Customer must minimise such information and establish an appropriate lawful basis and safeguards.

4. Develab processing obligations

4.1 Purpose limitation. Develab will process Customer Personal Data only to provide, operate, secure, troubleshoot, support and improve the subscribed Services in accordance with Customer's documented instructions, and to comply with law. Develab will not materially expand the purpose of Processor processing without Customer's instruction.

4.2 Confidentiality. Develab will ensure that personnel authorised to process Customer Personal Data are bound by confidentiality obligations, receive appropriate privacy and security training, and access the data only as necessary for their assigned duties.

4.3 Compliance assistance. Taking into account the nature of processing and information available to Develab, Develab will provide reasonable assistance for Customer's compliance with security, breach notification, Data Subject rights, data-protection impact assessments and prior consultation duties. Assistance beyond standard Service functionality or documentation may be charged at agreed professional-service rates unless caused by Develab's breach.

4.4 Records and regulatory cooperation. Develab will maintain records required of a Processor and, where required by law, cooperate with a competent supervisory authority regarding processing under these Terms. Develab may require requests to be made through Customer unless law or the authority requires direct engagement.

5. Security

5.1 Security programme. Develab will implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data against Personal Data Breaches, taking into account the state of the art, implementation costs, the nature, scope, context and purposes of processing, and risks to individuals. The current baseline measures are described in Schedule 2.

5.2 Security changes. Develab may update its safeguards to reflect technology, threats, law and Service changes, provided the overall level of protection is not materially reduced during a Subscription Term. No security measure guarantees absolute security.

5.3 Customer security responsibilities. Customer will use available security controls, maintain secure endpoints and integrations, protect credentials and keys, apply least privilege, review access, and maintain appropriate backups or exports for its business-continuity needs. Develab is not responsible for a breach caused by Customer systems, instructions, credentials or unauthorised third parties outside Develab's control.

5.4 Assurance reports. On written request and subject to confidentiality, Develab will make available then-current third-party certifications or summary assurance materials that it is lawfully permitted to share. Any reference to ISO/IEC 27001 applies only if the certificate is current and only to the certified entity, systems, locations and scope; certification does not by itself establish compliance with every privacy law.

6. Personal Data Breaches

6.1 Notification. Develab will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data. Develab will target an initial notice where feasible so Customer can assess mandatory deadlines, including Indonesia's controller notification period of no later than 3 × 24 hours where applicable.

6.2 Notice content. As information becomes available, Develab's notice will describe the nature of the breach, affected data and persons where known, likely consequences, containment or remediation measures, and an incident contact. Information may be provided in phases. Notice is not an admission of fault or liability.

6.3 Response. Develab will take reasonable steps to contain, investigate and remediate the breach and preserve relevant evidence. Customer is responsible for determining whether to notify individuals, regulators or others and for the content of those notices, except where law places a direct duty on Develab.

6.4 Customer incidents. Customer will promptly notify Develab of compromised credentials, unlawful instructions, unauthorised exports or other incidents that may affect the Services, and will cooperate in containment and remediation.

7. Subprocessors

7.1 General authorisation. Customer gives general written authorisation for Develab to engage Subprocessors to provide infrastructure, hosting, communications, monitoring, support, payment or other Service functions. Develab remains responsible for each Subprocessor's performance of data-protection obligations to the same extent as required by Applicable Data Protection Law.

7.2 Flow-down terms. Develab will conduct reasonable diligence and bind each Subprocessor by written obligations that provide protection materially equivalent to the relevant obligations in these Terms, having regard to the Subprocessor's services.

7.3 List and changes. Develab will maintain a current Subprocessor list at rideum.io/legal/subprocessors. Customer may subscribe to change notices. Develab will give prior notice of a new Subprocessor where practicable, except an emergency replacement may be notified as soon as reasonably possible.

7.4 Objections. Customer may object within the notice period on reasonable, documented data-protection grounds. The parties will work in good faith on a commercially reasonable alternative. If none is available, Develab may refrain from using the Subprocessor for Customer, suspend the affected feature, or permit Customer to terminate only the affected Service and receive a pro-rata refund of prepaid unused fees. This is Customer's sole remedy for a Subprocessor objection.

8. Data Subject requests

8.1 Customer responsibility. Customer is responsible for receiving, verifying and responding to Data Subject requests. Develab will not independently respond to a request concerning Customer Personal Data unless authorised by Customer or required by law.

8.2 Referral and assistance. If Develab receives such a request, it will forward it to Customer without undue delay where Customer can be identified. Taking into account the nature of processing, Develab will provide reasonable assistance through Service functionality or other appropriate technical and organisational measures.

8.3 Preservation and restrictions. Develab may preserve data or restrict action where reasonably necessary to verify authority, protect another person's rights, comply with legal holds or avoid compromising security. Customer will not instruct Develab to disclose data to an unverified requester.

9. International transfers and data location

9.1 Processing locations. Customer authorises processing in the countries listed in the approved Subprocessor list and Schedule 1. Customer acknowledges that support, resilience and infrastructure may involve more than one jurisdiction. Current hosting regions and support-access locations are set out in Schedule 1.

9.2 Transfer compliance. Each party will comply with restrictions on cross-border transfers applicable to its role. Customer is responsible for determining whether its disclosure to Develab is permitted; Develab will implement a required contractual transfer mechanism and reasonable supplementary safeguards within its control.

9.3 Transfer mechanisms. For a restricted transfer governed by the GDPR or UK GDPR, Schedule 4 applies. For Indonesian Personal Data, the parties will implement the lawful transfer basis and protections required by Indonesian law, including any adequacy, binding-protection, consent, assessment, recording or notification requirements applicable to the transfer.

9.4 Government requests. Unless prohibited by law, Develab will notify Customer of a legally binding government demand for Customer Personal Data. Develab will review the demand, disclose only data legally required, and use reasonable efforts to challenge an unlawful or disproportionate demand where there are reasonable grounds.

10. Audit and information rights

10.1 Standard assurance. Develab will provide information reasonably necessary to demonstrate compliance, ordinarily through completed questionnaires, policies, certifications, penetration-test summaries or independent audit reports. Customer will treat all assurance materials as Develab Confidential Information.

11. Return, deletion and retention

11.1 During the term. Customer may access and export Customer Personal Data using available Service functionality, subject to the Order. Customer is responsible for making timely exports and maintaining any legally required business records.

11.2 End of Services. Following termination or expiry, Develab will, at Customer's choice and subject to available functionality, return or delete Customer Personal Data within 30 days, unless law requires retention. Customer must request any special export before termination or within the stated retrieval period.

11.3 Backups and legal retention. Residual copies may remain in backups until overwritten under Develab's documented backup cycle and will remain protected and isolated from ordinary use. Develab may retain limited records where required for law, security, dispute resolution or financial compliance, and will delete or de-identify them when the retention purpose ends.

12. Liability and term

12.1 Liability. Each party's liability arising from these Terms is subject to the exclusions and aggregate cap in the EULA or applicable Order, except to the extent Applicable Data Protection Law prohibits limitation. Nothing in these Terms creates liability to a Data Subject beyond mandatory law.

12.2 Term. These Terms take effect with the Agreement and continue for as long as Develab processes Customer Personal Data. Obligations concerning confidentiality, security, breach cooperation, return or deletion, audits, transfers and liability survive to the extent necessary for retained data or enforcement.

12.3 Changes. Develab may update these online Terms prospectively to address legal, security or Service developments, provided material protection is not reduced during a Subscription Term without Customer's agreement unless required by law. Material changes will be notified under the EULA.

12.4 General. The governing law, dispute resolution, notices, assignment, severability, waiver, entire-agreement and counterpart provisions in the EULA apply. If there is no EULA, those provisions in the applicable Order apply.

Schedule 1 — Details of Processing

Processing detail	Description
Subject matter	Hosted operation, administration, support, security and maintenance of subscribed Rideum Suite modules: Bleustay, Bleudine and Bleudash.
Duration	For the Subscription Term plus the agreed retrieval, deletion and backup-retention periods.
Nature and purpose	Collection, recording, organisation, hosting, storage, consultation, transmission, configuration, retrieval, analysis, support, security, backup, export and deletion as needed to provide the Services on Customer's instructions.
Data Subjects	Customer personnel and users; hospitality guests, visitors and prospective guests; restaurant or outlet patrons; suppliers, contractors, business contacts and other persons whose data Customer submits.
Personal Data	Identity and contact details; account and authentication data; booking, stay, dining, order and service-preference information; communications and support records; transaction references; property, outlet and operational records linked to persons; device, usage, audit and security logs.
Sensitive data	Not intended unless expressly documented. Guest accessibility or dietary notes may reveal health or religious information; identity documents, payment data and children's information require minimisation and specific safeguards.
Frequency	Continuous or event-driven during ordinary use, with periodic backups, monitoring and support access.

Processing detail	Description
Locations	Primary hosting and disaster recovery within the Singapore region. Authorised support access occurs from Singapore and Indonesia.
Retention	Customer-configured retention during the Subscription Term. After termination, Customer Data is available for retrieval for 30 days, then deleted or anonymised, with backups deleted under the documented rolling backup cycle.
Controller rights	Customer may issue lawful instructions, configure access and retention, use available export/deletion tools, request assistance and exercise the audit rights in these Terms.

Schedule 2 — Technical and Organisational Measures

Control area	Baseline measure
Governance	Documented information-security and privacy responsibilities, risk assessment, policies, staff training and periodic control review.
Access control	Unique identities, role-based and least-privilege access, privileged-access controls, access review, prompt deprovisioning and multi-factor authentication where supported.
Confidentiality	Personnel confidentiality commitments and need-to-know access to production data and support cases.
Encryption	Encryption in transit using current secure protocols and encryption at rest for production data and backups where technically appropriate; managed keys and restricted key access.
Tenant and environment security	Logical tenant separation; controlled production access; separation of development, test and production environments; prohibition on using live Personal Data in non-production unless approved and protected.
Secure development	Change control, code review, dependency management, security testing and remediation processes proportionate to risk.
Vulnerability management	Asset inventory, patching, vulnerability scanning, severity-based remediation and periodic independent penetration testing for in-scope systems.
Logging and monitoring	Security and administrative event logging, time synchronisation, monitoring and alerting, protected log access and risk-based retention.

Control area	Baseline measure
Availability and resilience	Backups, recovery procedures, capacity and availability monitoring, incident response and periodic continuity or restoration testing.
Incident response	Documented detection, triage, containment, investigation, evidence preservation, remediation, communication and lessons-learned procedures.
Subprocessors	Risk-based due diligence, contractual security and privacy obligations, access limitation and ongoing review appropriate to the service.
Data lifecycle	Data minimisation support, retention and deletion processes, controlled exports, media disposal and backup expiration.
Assurance	ISO/IEC 27001 or other certification only if current and in scope; internal review and independent assurance materials where available.

Schedule 3 — Subprocessor Information

Develab maintains a current Subprocessor list at a stable URL identifying, at minimum, the legal name, service function, processing location, hosting region where relevant, data categories or purpose, and applicable transfer safeguard.

Field	Detail
List location	rideum.io/legal/subprocessors
Change notices	Subscribe by emailing compliance@develab.io; changes are also published on the Subprocessor page above.
Objection channel	compliance@develab.io — include your organisation name, the Subprocessor objected to, and the data-protection grounds for the objection.
Current providers	Cloud hosting and infrastructure (Singapore region); payment gateways such as Midtrans and Xendit; messaging providers (WhatsApp Business, email, SMS); AI and model providers, namely Anthropic, OpenAI and Google; and product analytics and error monitoring.

Schedule 4 — Restricted Transfer Addendum

S4.1 EEA transfers. Where Customer Personal Data subject to the GDPR is transferred to Develab in a country without an applicable adequacy decision, the European Commission Standard Contractual Clauses adopted by Decision (EU) 2021/914 apply by reference using Module Two (Controller to Processor), or Module Three where Customer is a Processor. The parties will complete the annexes, selected options, competent authority, governing Member State law and forum where they rely on the clauses.

S4.2 UK transfers. Where the UK GDPR restricts a transfer, the then-current UK International Data Transfer Addendum to the EU Standard Contractual Clauses, or another lawful UK mechanism agreed by the parties, applies.

S4.3 Other jurisdictions. The parties will execute or incorporate an additional mandatory transfer instrument where another Applicable Data Protection Law requires it. If a transfer instrument conflicts with these Terms, the transfer instrument controls for that transfer only.

S4.4 Transfer assessment. Each party will provide information reasonably necessary for a transfer-risk or equivalent assessment. Develab will implement reasonable supplementary technical and organisational measures within its control and notify Customer if it can no longer comply with the applicable mechanism.

Contact Us

For questions about this document, or to exercise any right described here, contact us:

Provider: Develab Pte. Ltd. (UEN 202402923E)

Email: sales@develab.io

Address: 10 Anson Road #10-11 International Plaza, Singapore 079903

Website: https://www.rideum.io