

Rowseta Data Processing Agreement

Version: 2026-10.2. Effective date: October 29, 2026
Last updated: October 29, 2026

BentoBits Inc.

1. Parties, application and roles

This Data Processing Agreement ("DPA") is between **BentoBits Inc.** ("Processor") and the organization identified in the accepted [Terms of Service](#) and account records ("Customer"). It applies to personal data processed by Processor on Customer's behalf in providing Rowseta (the "Service"). This data is "Customer Personal Data".

This DPA is incorporated into the Terms and binds the parties when Customer accepts the Terms. A separate signature is not required. It applies to paid and Evaluation use, including any required processing after access ends. Capitalized terms not defined here have the meanings given in the Terms. "Applicable Data Protection Law" means data protection and privacy law applicable to the relevant processing. "Personal data breach" has the meaning given by that law, including unlawful or accidental loss, destruction, alteration, unauthorized disclosure of or access to Customer Personal Data.

Customer acts as controller or, where it acts for another controller, as an authorized processor. In the latter case, Customer is responsible for having authority to appoint Processor as a sub-processor, issuing instructions consistent with the underlying controller's instructions, and coordinating obligations owed to that controller. References below to Customer's instructions and choices include those it is authorized to give on that controller's behalf.

This DPA does not govern personal information for which BentoBits independently determines the purposes and acts as controller, such as its own necessary account, billing-administration and legal records. The [Privacy Policy](#) describes that processing. Roles depend on actual purposes and applicable law; classifying information as a business record does not turn Customer-controlled content into BentoBits' independent data.

2. Processing details

Item	Details
Subject matter	Customer Personal Data processed to provide and support the Service as instructed.
Duration	During the account relationship and for the period necessary to complete the return or deletion required by section 9, including lawful retention of protected residual copies.
Nature and purposes	Receiving, storing, organizing, retrieving, querying, analyzing, displaying, transmitting, securing, supporting, backing up and deleting Customer Personal Data; administering instructed access; and processing LMS Account measurement data as described in section 3.

Item	Details
Personal data	Names, work email addresses, user and role identifiers, LMS identifiers, enrollments, course activity, grades, account configuration, relevant audit and diagnostic records, written reports and support content, and other data selected by Customer. Billing measurement includes Brightspace Course Access and Course Access Log extracts, the Brightspace Organizational Units data used to identify course offerings, derived user and course identifiers, UTC course-access days, per-user access counts and last-access days. Optional support media may include screenshots, images and recordings containing Customer Personal Data.
Data subjects	Customer's learners, instructors, staff, administrators, contractors and other people whose information Customer lawfully includes. Learners may include minors.
Processing frequency	According to Customer's use, configured synchronization, service administration and the scheduled measurement described in section 3.
Sensitive information	Customer determines the selected datasets and support content. Customer must establish the authority and safeguards required for any sensitive or specially protected information it supplies. The Service does not by itself establish compliance with a sector-specific legal regime.
Customer rights and duties	Customer determines the lawful purposes and basis of its processing, provides appropriate notices and obtains required permissions, supplies lawful documented instructions, manages its users and access settings, and handles individual rights and regulatory obligations with Processor's required assistance. These duties do not excuse Processor's own obligations.

3. Documented instructions

Processor will process Customer Personal Data only on Customer's documented instructions, including instructions concerning international transfers, unless applicable law requires other processing. In that case, Processor will inform Customer of the legal requirement before processing unless that law prohibits notice on important grounds of public interest.

The agreed instructions consist of this DPA, the Terms, Customer's authorized account settings and use of the Service, and other documented instructions accepted by Processor. An instruction requiring a material change to the Service may require agreement on feasibility and reasonable charges, but that process will not excuse or delay compliance with a mandatory duty. Processor will promptly inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law and may suspend the affected processing while the parties resolve it lawfully.

Customer instructs Processor to carry out processing reasonably necessary to operate, secure, maintain and troubleshoot the Service, including investigating service faults or security concerns identified by Processor without a Customer support request. This instruction permits only processing reasonably necessary for those purposes and does not authorize unrestricted inspection of Customer Personal Data or its use for unrelated purposes.

Customer authorizes Processor to perform proportionate automated checks of Service functionality, reliability and security using Customer Personal Data where synthetic or non-personal test information would not adequately perform the check. Such a check may process the Customer Personal Data necessary for the check, including query text and identifiable results, within the authorized environment. Any such check will preserve Customer-specific access boundaries and will not alter substantive Customer content or configuration, although normal execution metadata, caches and audit records may be created. Processor will retain only the diagnostic evidence necessary for the check and any resulting investigation. Processor will not begin such checks until these safeguards are in place.

Customer authorizes Processor to generate limited Organization-level operational measurements, including synchronization outcomes, sanitized error categories, query timings and aggregate sign-in counts, for monitoring, troubleshooting and capacity planning for the Service. These measurements exclude names, email addresses, individual user identifiers, query text, report results and learner-record content, and small counts are reduced or withheld where necessary to avoid identifying an individual. Processor will not use identifiable learner information for independent product-development purposes and will use only statistics that do not reasonably identify an individual for general product-improvement analysis. Organization-linked summaries are retained as stated in the Privacy Policy. Account purge removes ordinary Organization-linked summaries. Any residual information is retained only where it separately qualifies under the retention rules in section 9.

Customer instructs Processor to use the organization's stored Brightspace connection to check its LMS Account count daily without a Customer-initiated sync. This applies to Evaluation accounts after a completed sync and to active paid accounts during the 21 days before the subscription period ends, including accounts with cancellation scheduled. Locked, dormant, purged and failed-payment read-only accounts are excluded.

This measurement may download the latest full Course Access and Course Access Log extracts and later updates, use the Brightspace Organizational Units data synchronized for the Organization to identify course offerings, derive measurement records, and store dated count snapshots. The activity threshold is at least 10 distinct combinations of user identifier, course offering identifier, and UTC calendar day within the period from the count date minus 12 calendar months through the count date, including both dates. Only organizational units that the Organizational Units data identifies as type Course Offering are counted. Duplicate activity for the same user, course offering and day counts once toward that user's threshold. The LMS Account count is the number of qualifying users. These checks do not consume Evaluation sync credits or refresh analytical datasets. The Terms govern the commercial use of the resulting count.

Customer instructs Processor to perform pre-purchase LMS Account measurement where available, including before a completed sync. For this purpose, Processor may use Customer's stored Brightspace connection to obtain the latest available full extracts and applicable updates for Course Access, Course Access Log and Organizational Units and process them in separate billing storage. These checks may run automatically during connection setup or at Customer's request. They do not download other LMS datasets, consume Evaluation sync credits, or load or refresh analytical datasets. The resulting information remains subject to this DPA, including section 9.

Processor will not sell Customer Personal Data or use Customer-controlled LMS data to train machine-learning models. Providing an instruction under this section does not waive an individual's rights or determine a role contrary to the parties' actual processing purposes and Applicable Data Protection Law.

4. Confidentiality and personnel access

Processor will ensure that persons authorized to process Customer Personal Data are bound by appropriate confidentiality obligations or an applicable statutory duty of confidentiality. Access is limited to what is

necessary to carry out their duties.

Customer authorizes Processor's appropriately authorized personnel to access the minimum Customer Personal Data necessary to respond to Customer requests or to investigate service faults and security concerns identified by Processor. A separate Customer request, approval or routine notification is not required for each access within these documented instructions, unless Applicable Data Protection Law or an agreement with Customer requires otherwise. This does not limit breach-notification obligations under section 8.

Interactive support viewing of synced LMS data and other Organization records, such as people, reports and insight widgets, uses read-only, time-limited support sessions. Synced LMS data may include learner information. Authorized personnel may view the ticket submitter's name, email address and role, together with the Organization's plan, account status and Rowseta address, without opening a support session.

Necessary operational maintenance, security response and deletion may require access outside the interactive support facility. Such access remains subject to documented instructions, confidentiality, minimum necessary access and appropriate access records.

Processor will maintain access records appropriate to the relevant system and processing risk, sufficient to attribute personnel access and establish its purpose, timing and scope. Records may comprise linked system logs and support, maintenance or incident records. Purpose and scope are recorded once for each support session, investigation or maintenance task, and the related access activity is linked to that record. A new justification is recorded when the purpose or scope materially changes. Access outside the interactive support facility is documented through appropriate system records and an operational or incident record. Access records will not intentionally reproduce Customer content where references or other limited evidence are sufficient.

Personnel-access audit records are retained for two years, with source IP addresses removed after 30 days, subject to section 9 and applicable legal requirements. Incident files and technical service logs follow their own retention rules and are not governed by this paragraph. A verified authorized Customer representative may request the relevant access records relating to its Organization by contacting support@rowseta.com. Processor will provide the relevant records without undue delay, with proportionate redactions to protect other customers, unrelated personal information and security-sensitive details, without defeating Customer's audit rights or mandatory legal rights.

5. Security

Processor will implement appropriate technical and organizational measures required by Applicable Data Protection Law, taking account of the state of the art, implementation costs and the nature, scope, context, purposes and risks of processing. Measures will address confidentiality, integrity, availability, resilience, restoration and regular assessment of safeguards as appropriate to those risks.

Annex A describes the applicable categories of measures. Processor may update their implementation as technology and risks change, provided the changes do not materially reduce the overall protection of Customer Personal Data or breach Applicable Data Protection Law. No service availability percentage, response-time guarantee or recovery-time or recovery-point commitment is created by this DPA. That qualification does not excuse the required security and restoration measures or incident response.

6. Sub-processors

Customer gives general written authorization for Processor to engage the sub-processors identified in the provider register accompanying this DPA for the stated purposes. Annex B identifies the service providers,

purposes, relevant data and processing locations. Support email is received in a Gmail mailbox operated under Google's consumer terms; we do not claim that processor terms or a data processing agreement cover that mailbox. A provider acting solely as an independent controller is not a sub-processor for that independent processing.

Processor will give advance written notice of an intended addition or replacement, including enough information and time for Customer to meaningfully assess and object to the change on reasonable data-protection grounds before the new sub-processor begins the affected processing. Posting an updated list without giving the required notice is not sufficient. Notices will be sent through the account's designated legal-notice channel.

Customer must describe its objection promptly and sufficiently for Processor to assess it. The parties will work in good faith to address a legitimate objection, which may include additional safeguards or a commercially reasonable alternative. Processor will not commence the disputed processing contrary to applicable authorization requirements. If the parties cannot resolve the objection and Processor cannot reasonably continue the affected Service without the change, either party may terminate the affected Service. Processor will refund unused prepaid fees for the terminated portion as provided in the Terms and complete return or deletion under section 9. No prepaid-fee refund arises for free Evaluation use.

Processor will establish the contractual, security and transfer arrangements required by Applicable Data Protection Law for the affected processing. Where that law requires Processor to pass data-protection obligations to a sub-processor, Processor will make those obligations binding before the affected processing begins. Processor remains responsible to Customer for its sub-processors' performance of those obligations. Sub-processing does not remove any responsibility that applicable law places directly on Processor.

7. Individual requests

Taking account of the nature of processing, Processor will assist Customer through appropriate technical and organizational measures, insofar as possible, in responding to requests to exercise rights under Applicable Data Protection Law.

Processor will promptly inform Customer of a request received directly concerning Customer Personal Data and will not respond substantively without Customer's documented instruction, except as required by law. Processor may acknowledge receipt and direct the individual to Customer. Customer is responsible for deciding the response, subject to its own legal duties and the assistance required from Processor.

8. Breaches and compliance assistance

Processor will notify Customer **without undue delay** after becoming aware of a personal data breach affecting Customer Personal Data. Notice will be sent to Customer's designated account contact and will describe, to the extent then known, the nature of the breach; affected data and individuals; likely consequences; measures taken or proposed to address and mitigate it; and a contact for further information. Information may be provided in phases as it becomes available without undue further delay. An incomplete initial investigation is not a reason to delay required notice.

Processor will take appropriate steps to contain, investigate and mitigate the breach and cooperate with Customer. Notification does not itself admit liability. Customer remains responsible for notices to individuals and authorities for which it is legally responsible; Processor remains responsible for its own statutory duties.

Taking account of the nature of processing and information available to it, Processor will assist Customer with obligations concerning security, breach notification, data protection impact assessments and consultation with

a supervisory authority where required by Applicable Data Protection Law.

9. Return, deletion and residual copies

At the end of the relevant processing services, Processor will, at Customer's choice, return or delete Customer Personal Data and delete existing copies, unless applicable law requires storage. Customer may use available export and deletion functions or communicate its choice to **support@rowseta.com**. An authorized account-deletion request is a documented instruction to delete, subject to any lawful return instruction given with that request.

For self-serve Organization deletion, Customer instructs Processor to suspend ordinary Service access and syncing immediately and schedule deletion to begin after a seven-day cancellation period. An authorized Owner may withdraw the scheduled deletion instruction before the deadline shown when the request is confirmed. Unless withdrawn, Processor will commence deletion promptly after that deadline through the processes described in this section. Customer may contact support@rowseta.com to request earlier deletion or communicate a required return instruction. Processor will handle verified instructions for earlier deletion without undue delay, subject to applicable lawful preservation and return obligations.

Processor will provide a reasonable means of implementing a required return instruction and will then delete its remaining copies as required. Customer does not need continuing interactive access to communicate or exercise this choice. Return or deletion after access ends is handled through a support-led process on request to support@rowseta.com. Evaluation may be discontinued under the Terms without a guaranteed notice period, storage term or additional interactive export window. That discretion does not release Processor from this section or permit irreversible deletion that defeats a return choice Processor is legally or contractually required to honor. Processor need not restore information already lawfully deleted under a completed instruction or applicable agreed retention rule.

During processing, raw billing extracts are deleted after successful processing. Publication of a newer count snapshot triggers cleanup of superseded compact access files and per-user snapshots no longer required for processing or current billing and report snapshots. Failed cleanup is retried during later successful runs. Deleting an analytical dataset does not itself delete the separate billing measurement files. Remaining measurement files and account-linked snapshot records are removed through account purge, subject to a lawful and separately justified minimal record.

Backup copies are removed through the configured backup retention and cleanup lifecycle. Processor will protect residual copies, restrict their processing to necessary storage, security, recovery or legal compliance, and reapply deletion suppression for Organization purge and support media if data is restored. Temporary working data, technical logs and support-system copies containing Customer Personal Data are also subject to this section and applicable retention rules. A processing system's cleanup behavior does not create an exemption from an applicable deletion obligation.

Customer authorizes Processor to create limited temporary copies of Customer Personal Data where reasonably necessary to investigate or resolve service faults, including faults identified by Processor, to provide necessary customer support or to investigate security incidents. Copies must remain within approved, access-controlled environments and comply with applicable location, transfer and security requirements.

Processor will limit the information copied, document its purpose and retention, and delete it when no longer necessary, subject to applicable preservation obligations and Customer instructions. Separate Customer approval is required where the proposed processing falls outside these agreed instructions or an applicable legal or contractual requirement requires it.

If law requires continued storage, Processor will retain only the required data for the required purpose and duration, protect it under this DPA, and delete it when the legal requirement ends. Independently controlled minimal transaction, agreement or compliance records are governed by applicable law and the Privacy Policy; that distinction cannot be used to retain unnecessary LMS content. BentoBits independently determines the purposes of the limited Evaluation allowance records described in the Privacy Policy. These records contain hashed identifiers derived from owner email addresses and Brightspace instance addresses, usage counts and necessary dates, and are used only to administer Evaluation allowances and prevent their misuse. Their retention after Organization deletion is limited as described in the Privacy Policy. This provision does not authorize retention of Customer-controlled LMS content or reduce Processor's return and deletion obligations for Customer Personal Data. Identifier-only technical suppression markers are kept indefinitely in Canada for Organization purge and support-media deletion. Processor will provide reasonable confirmation of completed return or deletion on request. An acknowledgment that a deletion request has been accepted does not constitute confirmation of completion. Any completion confirmation will identify its scope and any remaining copies or records retained under this section, including their applicable retention arrangements.

10. Information, audits and assistance costs

Processor will make available information necessary to demonstrate compliance with this DPA and obligations applicable to Processor, and will allow and contribute to audits, including inspections, conducted by Customer or an auditor it mandates.

The parties will ordinarily begin with relevant documentation and written questions. Where further verification is needed, they will coordinate proportionate scope, reasonable scheduling, confidentiality and security arrangements. Customer's auditor must have appropriate competence and confidentiality duties. Audits must protect other customers' information and avoid unnecessary disruption. These arrangements do not prohibit a legally required inspection, restrict a supervisory authority, or prevent necessary urgent verification after a breach or credible compliance concern. There is no fixed annual audit limit.

Routine compliance information and ordinary assistance are included in the Service. Processor may propose reasonable charges for additional work that is unusually extensive, repetitive or requires bespoke resources, with scope and charges agreed in advance. Charges will not be imposed for remedying Processor's own breach and may not deter, obstruct or condition compliance with mandatory rights or assistance obligations. Customer is responsible for its own independent auditor's fees except where applicable law requires otherwise.

11. Locations and international transfers

Global is the only storage location currently offered for the stored content identified in the Privacy Policy, with no guaranteed storage location. Processing and metadata are configured in Canada. Cloudflare's network terminates TLS and proxies web traffic worldwide, and providers may process information in other countries as identified in Annex B. Temporary working data can be processed outside the selected content-storage jurisdiction.

Processor will transfer Customer Personal Data to a third country or international organization only on documented instructions and in compliance with applicable transfer requirements. Where a transfer can lawfully rely on an applicable adequacy decision, the scope and conditions of that decision must cover the actual recipient and processing. Adequacy for one transfer does not by itself resolve onward transfers.

Where Standard Contractual Clauses or another customer-specific mechanism is required, the necessary mechanism, annexes, assessments and supplementary safeguards must be completed before the affected

processing begins. This DPA does not select an SCC module, complete customer-specific terms or represent that a transfer assessment has been completed. If a required lawful arrangement is unavailable, the affected processing must not proceed. The parties will cooperate to resolve the issue and, if necessary, end the affected processing consistently with the Terms and section 9.

12. Liability, precedence and duration

The limitations and exclusions of **BentoBits'** liability in the Terms apply to claims under or relating to this DPA, including ordinary contractual confidentiality, privacy and security claims, to the extent legally permitted. This DPA creates no separate higher cap, uncapped contractual exception or supplier indemnity. The Terms determine the applicable paid-term or free/Evaluation cap and allocation of claims.

Nothing in this DPA or the Terms limits an individual's rights or a regulator's powers, or excludes or restricts an obligation or liability to the extent it cannot lawfully be limited. Where an applicable mandatory transfer mechanism requires different liability rules, those rules prevail, including for liability and recourse between the parties to the extent required by that mechanism. A customer indemnity or other term must not be used to defeat those mandatory rules.

This DPA controls over conflicting Terms concerning the parties' personal-data processing obligations. The Terms continue to govern commercial matters and limitations of liability, subject to the preceding paragraphs. Applicable mandatory transfer terms control over both documents for the processing they govern. The public Privacy Policy and Security notice do not amend this precedence.

This DPA continues for as long as Processor retains Customer Personal Data subject to it. Obligations concerning retained data, accrued rights and provisions intended to survive continue as necessary after Service access ends.

Annex A. Technical and organizational measures

The following describes measures for the Service. Measures apply to the relevant processing environment and are implemented according to risk. The [Security and Data Handling](#) notice provides operational context; it does not silently expand this annex into an availability or recovery guarantee.

Area	Measures
Organization separation and access	Organization-scoped application access and permissions; organization-specific storage boundaries; validation of identity and authorization before access to Customer content.
Personnel access	Confidentiality obligations; role-appropriate privacy and security training; access limited to authorized duties; read-only, time-limited interactive support sessions; recorded reasons and access activity; documented operational access outside support sessions; and procedures for reviewing access and removing it when no longer required.
Transport and credentials	HTTPS for application access; protected service connections; application encryption of stored LMS credentials; secrets kept out of ordinary user-facing responses and access limited to necessary operations.

Area	Measures
Stored information	Provider-managed encryption for content storage and platform volumes; protected metadata backups; configured storage jurisdictions for the applicable content categories.
Monitoring and incidents	Relevant service and access logging; restriction of access to logs; investigation and response procedures appropriate to incidents; breach notification and cooperation under section 8. Logs can contain personal data and require protection accordingly.
Availability and restoration	Platform-metadata backups and procedures for restoring information as appropriate to the processing risks; protection of backups and reapplication of deletion suppression for Organization purge and support media following restoration.
Retention and disposal	Dataset and account deletion procedures; billing measurement cleanup; backup and log rotation; support-media deletion; restricted retention of legally required information.
Ongoing assessment	Review of access and safeguards and regular testing or evaluation appropriate to the processing risks, with correction of identified material deficiencies.

Annex B. Service providers

The following service providers support Rowseta. A provider acting as an independent controller is not a sub-processor for that independent processing. The Gmail mailbox is operated under Google's consumer terms, without a claim of processor terms or a data processing agreement covering it.

Service provider	Purpose	Data	Location
Fly.io, Inc.	Application and worker hosting, metadata volumes and volume snapshots	Connected LMS data, account metadata and service records	Toronto, Canada; snapshot storage location is not specified
Cloudflare, Inc.	Cloudflare R2 content storage	Analytical files, billing measurement files and in-app report media	Global, with no guaranteed storage location
Cloudflare, Inc.	Network, Email Routing and Turnstile	Web traffic, forwarded support email and bot-protection information	Worldwide
Amazon Web Services Canada, Inc.	AWS S3 platform-metadata backups and deletion-control records	Platform metadata and identifier-only deletion markers	ca-central-1, Canada
Amazon Web Services Canada, Inc.	AWS CloudWatch Logs technical service logging	Identifiers and diagnostic values from customer processing	ca-central-1, Canada

Service provider	Purpose	Data	Location
Plus Five Five, Inc. (Resend)	Transactional emails and support notifications	Recipients, Organization metadata and diagnostic details	Sending region us-east-1; this does not specify a storage location
Google LLC (Gmail)	Gmail mailbox under Google's consumer terms	Support email, forwarded notifications and information supplied by senders	May process in the United States and other countries
Stripe Payments Canada, Ltd.	Payment, invoice and subscription administration	Billing contacts, Organization details and purchase measurement metadata	May process in the United States and other countries