BUBURUZA

Buburuza Data Processing Addendum

LAST UPDATED	5 November 2026
VERSION	DPA-2026-11-05

This Data Processing Addendum (“**Addendum**”) is between the business customer (“**Customer**”) and the Buburuza company that provides its business account (“**Buburuza**”): **Buburuza Payments LLC** for U.S. businesses and **Buburuza AI Inc.** for other businesses. It forms part of the Customer Agreement between them (the “**Agreement**”) and applies to every business customer from its acceptance of the Customer Agreement or the API Terms. A copy countersigned by Buburuza is available on request at dpo@buburuza.com.

1 Definitions

Words defined in the Agreement have the same meaning here. In addition:

- **Customer Personal Data** means personal information that Customer provides, or makes available through the Services, about its own customers, payers, payees, employees, contractors and contacts, and that Buburuza processes on Customer’s behalf under section 2.1.
- **Data Protection Laws** means the privacy and data-protection laws that apply to that processing, which may include Canada’s Personal Information Protection and Electronic Documents Act, Quebec’s Act respecting the protection of personal information in the private sector (“**Law 25**”), U.S. state privacy laws such as the California Consumer Privacy Act, the EU and UK General Data Protection Regulation (“**GDPR**”) and the Swiss Federal Act on Data Protection.
- **Security Incident** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data, including a “confidentiality incident” under Law 25.
- **Subprocessor** means a service provider that Buburuza engages to process Customer Personal Data.
- **Controller**, **processor**, **service provider**, **data subject** and **processing** have the meanings given in the applicable Data Protection Laws.

2 Roles

1. **Buburuza as processor.** Buburuza processes Customer Personal Data as Customer’s processor or service provider for the content Customer puts into invoices, payment requests and payment pages; Customer’s own records of its customers, payers, payees and contacts; the team roles and budgets Customer configures; data sent through the API; and exports and connected apps that Customer uses, as described in Annex 1.
2. **Buburuza as independent controller.** Buburuza is an independent controller, and this Addendum does not apply, when it processes personal information for its own purposes: opening and running accounts, verifying identity and ownership, anti-money-laundering, sanctions and fraud checks (including on payers, as the Payer Terms and Privacy Notice explain), executing and recording payments, complying with legal and regulatory duties, handling complaints and

disputes, security, and its own relationship with people who hold their own Buburuza account or card, including end users who are Buburuza's customers under a Partner Programme Agreement. Card data is processed by Buburuza Payments LLC as controller under the Buburuza Card Terms. The Buburuza Privacy Policy describes that processing.

3. **Partners.** Banks, card issuers, payment and stablecoin partners, bank-linking providers and the providers of apps Customer connects, other than the WhatsApp messaging service listed as a Subprocessor, process information as independent controllers under their own terms. They are not Subprocessors.
4. **Customer's responsibilities.** Customer is responsible for having a lawful basis for the Customer Personal Data it gives Buburuza, for giving people the notices the law requires, and for its instructions complying with Data Protection Laws. Customer must not send special-category or sensitive information through the Services unless the Services are designed for it.

3 Instructions

Buburuza processes Customer Personal Data only on Customer's documented instructions. The Agreement, this Addendum and Customer's use and configuration of the Services are Customer's complete instructions when this Addendum starts to apply; further instructions must be in writing and consistent with the Agreement. Buburuza tells Customer if, in its opinion, an instruction infringes Data Protection Laws, and may then decline to follow it. Buburuza may process Customer Personal Data where the law requires it; it tells Customer before doing so unless the law prohibits that.

4 U.S. service-provider terms

Where U.S. state privacy laws apply, Buburuza: (a) does not sell or share Customer Personal Data, as those terms are defined in those laws; (b) does not retain, use or disclose it for any purpose other than providing the Services under the Agreement, or outside the direct business relationship with Customer, except as those laws allow; (c) does not combine it with personal information it receives from other sources, except as those laws allow; (d) complies with those laws and provides the same level of privacy protection they require; and (e) tells Customer if it can no longer meet its obligations. Customer may take reasonable steps to stop and remedy unauthorised use. Buburuza certifies that it understands these restrictions.

5 Confidentiality and security

1. Buburuza ensures that people authorised to process Customer Personal Data are bound by confidentiality and receive appropriate training.
2. Buburuza implements and maintains the technical and organisational measures in Annex 2, appropriate to the risk. It may update them if the overall level of protection is not reduced.

6 Subprocessors

1. Customer gives Buburuza general authorisation to engage Subprocessors. The current list is published on the Buburuza Subprocessors page.
2. Buburuza gives at least 30 days' notice by email, or by a notice on that page that Customer can subscribe to, before adding or replacing a Subprocessor. Customer may object on reasonable

data-protection grounds within that period. If the parties cannot resolve the objection in good faith, Customer may end the affected Services without penalty and receive a refund of prepaid fees for the unused period.

3. Buburuza imposes on each Subprocessor, by written contract, data-protection obligations that are no less protective than this Addendum, and remains responsible to Customer for its Subprocessors' performance of those obligations.
4. In an emergency affecting security or continuity of the Services, Buburuza may replace a Subprocessor with shorter notice, and tells Customer as soon as possible.
5. Where the Standard Contractual Clauses apply, we notify the Customer directly in writing at least 30 days before adding or replacing a Subprocessor. We use a shorter period only under an arrangement agreed in advance with the Customer that meets the applicable transfer requirements. Customer's objection and termination rights under section 6.2 remain.

---

7 Data subjects' requests

Taking into account the nature of the processing, Buburuza helps Customer, by appropriate technical and organisational measures, to respond to requests from people exercising their rights. If Buburuza receives a request about Customer Personal Data, it refers the person to Customer and does not respond itself, except to confirm the referral or where the law requires.

---

8 Security Incidents

1. Buburuza notifies Customer without undue delay, and in any case within 48 hours, after becoming aware of a Security Incident affecting Customer Personal Data.
2. The notice describes, as far as then known, the nature of the incident, the categories and approximate number of people and records concerned, the likely consequences, and the measures taken or proposed. Buburuza provides further information as it becomes available, takes reasonable steps to contain and remedy the incident, and keeps a record of it.
3. Notifying a Security Incident is not an admission of fault. Customer decides whether to notify regulators and affected people where the incident concerns its own data; Buburuza cooperates.
4. **Québec.** Where Québec law applies to processing on Customer's behalf, Buburuza notifies Customer's person in charge of privacy without delay of any breach or attempted breach of a confidentiality obligation and permits that person to verify compliance. These duties take priority over the ordinary notice and audit periods in sections 8.1 and 12.

---

9 Assistance

Buburuza provides reasonable assistance, taking into account the information available to it, with Customer's privacy impact assessments, data protection impact assessments and any prior consultation with a regulator relating to the Services.

---

10 Transfers outside the country of collection

1. Buburuza and its Subprocessors may process Customer Personal Data in the United States, Canada and the other countries stated on the Subprocessors page.

2. **Quebec.** Before communicating Customer Personal Data outside Quebec, Buburuza carries out, and makes available to Customer on request, the assessment required by section 17 of Law 25, and relies on written agreements that take account of its results.
3. **EEA, United Kingdom and Switzerland.** Where GDPR or the Swiss Act applies to a transfer of Customer Personal Data to a country without an adequacy decision, the parties agree to the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), with the UK Addendum and the Swiss adaptations where relevant. They are incorporated by reference, with Annex 1 and Annex 2 of this Addendum completing their appendix. Clause 7 (docking) and the optional wording in clause 11 do not apply; clause 9 option 2 (general authorisation) applies with the notice period in section 6.2; the governing law and courts under clauses 17 and 18 are those of Ireland. For transfers subject to UK law, the parties agree to the International Data Transfer Addendum issued by the UK Information Commissioner: Table 1 is completed by the party details in Annex 1, Table 2 by the Module Two Clauses and the choices above, Table 3 by Annexes 1 and 2 and the Subprocessors page, and for Table 4 neither party may end the Addendum under its section 19. Before a restricted transfer begins, we document, with the Customer as applicable, the assessment required for its actual destination and safeguards. We make that assessment available to the Customer on request. If the Clauses conflict with this Addendum, the Clauses prevail.

---

11 Return and deletion

When processing services end, Buburuza returns or deletes Customer Personal Data at Customer's choice and deletes existing copies, subject to legally required retention. The 30-day export window is available if Customer chooses return. Buburuza completes deletion within 90 days, including copies held by Subprocessors, and follows any shorter deadline required by applicable law. Information that Buburuza keeps as an independent controller under section 2.2, such as payment and anti-money-laundering records, is governed by the Privacy Policy and the law, not by this section. Backups awaiting secure deletion stay isolated, are deleted on their normal cycle and are not restored for any other use.

---

12 Audits

1. Buburuza makes available on request the information reasonably necessary to show that it meets this Addendum, including summaries of its security policies and any independent audit reports or certifications it holds, under confidentiality.
2. If that information is not enough to meet a requirement of Data Protection Laws or a regulator, Customer may audit Buburuza's compliance with this Addendum, itself or through an independent auditor bound by confidentiality, no more than once a year, on at least 30 days' notice, during business hours and without disrupting the Services or other customers. Customer bears its own costs. An audit does not give access to other customers' data, to Buburuza's privileged material or to its Subprocessors' facilities except as their contracts allow.

---

13 Liability and precedence

Each party's liability under this Addendum is subject to the limits in the Agreement, except where Data Protection Laws do not allow those limits. If this Addendum conflicts with the Agreement on

the processing of Customer Personal Data, this Addendum prevails. The Agreement's governing law and courts apply, except as section 10.3 provides.

14 Language

This Addendum is available in English and French. Customers in Quebec receive the French version first and are bound by it, unless they expressly choose the English version after receiving it.

Countersigned copy (optional)

This Addendum applies without signature. A Customer that wants a countersigned copy can sign below and send it to dpo@buburuza.com.

CUSTOMER	BUBURUZA
Legal name:	Buburuza Payments LLC / Buburuza AI Inc. (delete one)
Name and title:	Name and title:
Signature:	Signature:
Date:	Date:
Contact for privacy notices:	Privacy contact: dpo@buburuza.com

Annex 1 — Description of the processing

ITEM	DESCRIPTION
Parties' roles	Customer: controller. Buburuza: processor or service provider. For EU and UK transfers, Customer is the data exporter and Buburuza the data importer.
Party details	Data exporter: Customer, at the legal name, address and contact recorded in its business account. Data importer: Buburuza Payments LLC, 407 East Ayre Street #1451, Wilmington, Delaware 19804, United States, or Buburuza AI Inc., Bentall II, 555 Burrard Street, Office 03-109, Vancouver, British Columbia V7X 1M8, Canada, as applicable; contact: dpo@buburuza.com.
Destination countries	United States, Canada and the other countries stated on the Subprocessors page.
Data subjects	Customer's customers and payers; payees and recipients; Customer's employees, contractors and team members, for the roles and budgets Customer configures; Customer's contacts.
Categories of data	Names, business names, email addresses, phone numbers, postal and billing addresses; invoice, payment-request and line-item details; bank account or wallet details of payees; payment status and history for Customer's requests; team roles and budgets Customer configures; messages and files Customer adds; data sent through the API or webhooks; files saved to apps Customer connects.

ITEM	DESCRIPTION
Sensitive data	None intended. Customer must not send special-category data unless the parties agree otherwise in writing.
Purpose	Providing the Services that Customer uses under section 2.1: issuing and sending invoices and payment requests, showing payment pages, keeping recipient lists, applying the team roles and budgets Customer configures, API and webhook delivery, exports and connected apps, and related support.
Nature of processing	Collection, storage, organisation, retrieval, use, transmission, display to authorised users, and deletion.
Frequency	Continuous while Customer uses the Services.
Duration and retention	For the term of the Agreement and the deletion period in section 11.
Subprocessors	As listed on the Subprocessors page, for the purposes stated there.
Competent supervisory authority (EU transfers)	The authority of the EU member state where Customer is established or, if none, where its EU representative is established.

Annex 2 — Technical and organisational measures

1. **Encryption.** Data is encrypted in transit using TLS 1.2 or higher, and at rest using industry-standard encryption.
2. **Access control.** Access to production systems and Customer Personal Data is limited to authorised staff with a business need, granted on least-privilege principles, protected by multi-factor authentication and reviewed regularly. Access is removed promptly when no longer needed.
3. **Customer controls.** Roles and permissions for account users, approval rules, passkeys or two-factor authentication, API key scopes and webhook signatures.
4. **Logging and monitoring.** Security-relevant events are logged and monitored, and logs are protected from tampering.
5. **Secure development.** Code review, separation of test and production environments, dependency and vulnerability management, and a public bug bounty programme.
6. **Vendor management.** Subprocessors are assessed for security and privacy before engagement and reviewed periodically.
7. **Incident response.** A documented incident response plan with defined roles, escalation and notification steps, tested periodically.
8. **Business continuity.** Backups, disaster-recovery and business-continuity plans, tested periodically.
9. **People.** Confidentiality obligations and security and privacy training for staff with access to personal information.
10. **Data minimisation and deletion.** Collection limited to what the Services need, and deletion under documented retention schedules.