Bizmitra

Data Processing Addendum

Data Processing · Version **v2.0** · Effective **Sep 6, 2026** · Last updated **Sep 6, 2026**

Processor terms, the Workforce schedule and the international-transfer schedules.

Legal entity	**Drushtant Infoweb Private Limited**
Registered office	51, Kailash Complex-A, Near Gundala Gate, Gondal - 360311, Gujarat, India

Interpretation. This document describes Bizmitra’s current service and current-law position as at the date above. Mandatory law prevails where it cannot lawfully be varied. Read it with the other Bizmitra legal documents referenced in it.

1. Scope and parties

This Data Processing Addendum ("DPA") forms part of the Bizmitra Master Services Agreement, Online Terms of Service, Order Form or other written agreement between Bizmitra and the customer identified in that agreement ("Customer"). It applies to Personal Data that Bizmitra processes on behalf of Customer in providing the contracted Services.

Customer is the controller, employer, data fiduciary, data manager or equivalent responsible party under applicable law. Bizmitra is the processor/service provider acting on Customer’s documented instructions, except for limited account-administration, billing, security, legal-compliance and direct-support data that Bizmitra independently controls under the Global Privacy Notice.

2. Definitions

"Customer Personal Data" means Personal Data processed by Bizmitra on Customer’s behalf. "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, to the extent defined by applicable law. "Subprocessor" means a third party engaged by Bizmitra to process Customer Personal Data on Bizmitra’s behalf.

3. Customer instructions and purposes

Bizmitra will process Customer Personal Data only to provide, secure, maintain and support the Services, in accordance with the Agreement, Customer configuration/actions and documented support/API instructions, unless law requires otherwise.

Bizmitra will not sell Customer Personal Data or use Customer ERP/CRM/Workforce data for unrelated advertising.

Workforce employee data is not submitted to OpenAI or routed through Bizmitra’s Germany AI environment under the current standard Workforce service.

Limited sales forecasting may process only the month/year/total-sales summary described in the Privacy Notice and Schedule 1; it must exclude customer/vendor/ledger identities and Workforce data.

4. Customer responsibilities

Customer is responsible for the legality, accuracy and source of Customer Personal Data, including Tally-synchronised/imported data.

Customer will identify and document the lawful basis/authority for its processing and will provide required employee/customer/vendor notices.

Customer will obtain and retain evidence of any consent, explicit consent, permit, regulator approval, employment consultation or international-transfer approval required by the law applicable to Customer.

Customer will not instruct Bizmitra to process data that must be localised or requires a permit/approval unless those conditions have been satisfied and the deployment is covered by the Agreement.

Customer will manage user roles, remove former users, protect credentials/endpoints and ensure any consent relied upon is not obtained through unlawful coercion.

Customer will provide notices/consent in a language and form reasonably understandable to the affected workforce where required.

5. Confidentiality and personnel

Bizmitra will limit access to Customer Personal Data to personnel who require it for their duties and who are subject to confidentiality obligations. Bizmitra remains responsible for its personnel’s handling of Customer Personal Data to the extent required by applicable law and the Agreement.

6. Security measures

TLS-protected service and API traffic.

Role-based access controls and logical tenant scoping/separation.

Restricted production administration, firewalling, monitoring, patching and backup processes.

Application/security logs and financial audit controls appropriate to the Service.

Incident triage, containment, recovery and documented cooperation with Customer.

Security is shared. Customer controls its user permissions, devices, credentials, uploaded content and third-party integrations.

7. Subprocessors

Customer gives Bizmitra general authorisation to use Subprocessors necessary to provide the Service. Bizmitra will maintain a current Subprocessor & Data Location List and will impose appropriate confidentiality/data-protection obligations on Subprocessors that process Customer Personal Data. Where the Agreement or applicable law requires prior notice of a material new Subprocessor, Bizmitra will provide such notice and a reasonable mechanism to raise a bona fide data-protection objection.

OpenAI is not a Subprocessor for the current standard ERP/CRM/Workforce Customer Personal Data processing. OpenAI is used for the separate public guest chat and may become a Customer-data Subprocessor only for a separately disclosed/activated AI feature covered by the relevant product terms and transfer analysis.

8. Data-subject requests

If Bizmitra receives a request relating to Customer-controlled data, Bizmitra may direct the requester to Customer and will provide reasonable assistance, taking into account the nature of processing and information available to Bizmitra. Customer remains responsible for determining the legal response, identity verification and deadline unless law directly places that duty

on Bizmitra.

9. Personal Data Breaches

Bizmitra will notify Customer without undue delay after confirming a Personal Data Breach affecting Customer Personal Data where notice is required under applicable law or the Agreement. Bizmitra will provide reasonably available information concerning the nature of the incident, affected data, containment and remediation. Customer is responsible for regulator/data-subject notifications as controller unless law directly requires Bizmitra to notify.

10. Assistance, DPIAs and regulator cooperation

Taking into account the nature of processing and information available, Bizmitra will provide reasonable assistance with Customer’s legally required privacy/security assessments, regulator inquiries and consultations relating to Bizmitra processing. Bespoke legal/compliance work beyond standard documentation may be subject to reasonable fees where permitted.

11. Return, export and deletion

During an active subscription, Customer may export data using available Service functions. After termination/expiry, Bizmitra will make Customer data available for export for 30 days where technically available and legally permitted, unless the Order Form states a different period. After that period, Bizmitra may delete or de-identify Customer Personal Data from active systems, subject to legal holds, security logs, financial/audit integrity, statutory retention and ordinary backup rotation. Retained processor data will be restricted from ordinary business use.

A deletion instruction does not require Bizmitra to corrupt a legally required accounting/audit trail or delete information that Bizmitra must retain by law. Customer is responsible for identifying the statutory recordkeeping periods applicable to its business records.

12. Audit

On reasonable written request, Bizmitra will provide information reasonably necessary to demonstrate compliance with its processor obligations, subject to confidentiality and security restrictions. Customer will first use available documentation. Any audit must be proportionate, coordinated in advance, avoid exposure of other customers’ data and avoid unreasonable disruption. On-site audits may be subject to reasonable cost recovery unless required due to a confirmed material breach by Bizmitra or mandatory law.

13. International transfers

Customer authorises the processing locations identified in the Agreement, Privacy Notice and this DPA. If applicable law requires additional transfer terms, the relevant Schedule below applies. Customer will not activate a country/data category that requires localisation, regulator approval or a transfer mechanism not yet implemented without prior written agreement.

14. Liability allocation

The liability limits in the governing customer agreement apply to this DPA except to the extent mandatory law requires otherwise. Customer will indemnify Bizmitra against third-party claims and reasonable regulatory/legal costs arising from Customer’s unlawful collection, failure to provide required notice/consent/permit/transfer approval, unlawful imported/Tally

data, or unlawful Customer instruction, except to the extent caused by Bizmitra's breach of this DPA or applicable law.

Schedule 1 - Processing details

Item	Description
Subject matter	Cloud ERP, CRM, accounting, inventory, Workforce employee self-service, Tally-connected, developer/API and related business-processing services ordered by Customer.
Duration	Subscription term plus agreed export/deletion, statutory retention, backup rotation and legal-hold periods.
Data subjects	Customer personnel, employees/workers, Customer customers/buyers, suppliers/vendors/contacts, authorised users and persons represented in accounting/CRM records.
Data types	Identity/contact data; employment, leave/attendance and payslip/payroll information where enabled; statutory identifiers where applicable; optional bank/payment details only where an enabled workflow requires them; business/transaction/ledger data; invoices/orders/receipts/payments; device/user/audit logs.
Sensitive/special data	Only where expressly enabled and legally permitted. Customer must satisfy any special permit, consent, localisation or regulator requirements before use.

Processing	Location / restriction
ERP/CRM production and ordinary backups	Mumbai, India - Akamai Connected Cloud / Linode.
Workforce production and ordinary backups	Mumbai, India.
Workforce/ERP Customer Personal Data to OpenAI	None under the current standard service unless a separately disclosed AI feature is ordered/activated.
Sales forecasting	Only month, year and total-sales summary metrics may be sent to Hetzner, Germany; identifying customer/vendor/ledger and Workforce data are excluded.
Public /vi/public_chat	Separate Bizmitra-controlled guest service; not Customer ERP/Workforce processing under this DPA unless expressly incorporated by an Order Form.

Schedule 2 - Workforce Processing Schedule

This Schedule applies when Customer enables Workforce, employee self-service, payslip, leave, attendance or related HR functions.

Employees cannot self-register. Customer/employer creates or approves the employee record and remains responsible for the employment relationship and lawful basis.

Customer will provide the Bizmitra Workforce Employee Privacy Notice at or before first login and keep it available later. For already-active employees, Customer will promptly provide the current notice and maintain a record of delivery/acknowledgement where appropriate.

Workforce production personal data and ordinary backups are hosted in Mumbai, India. Under the current service, Workforce data is not sent to OpenAI or Bizmitra's Germany AI environment.

Device biometric unlock is performed locally through the operating system. Bizmitra does not receive/store fingerprint or face images/templates/biometric identifiers; a boolean biometric-enabled setting may be stored.

Bank/payment details are processed only if Customer activates a workflow that actually requires them. In the current Bahrain/Oman/UAE self-service configuration described to Bizmitra, Customer performs salary processing/transfer in its own payroll system and does not store employee bank details in Bizmitra; Bizmitra stores payslip/salary information needed for employee access.

Customer will avoid enabling country-irrelevant fields. India-specific PAN/UAN fields should be hidden outside India unless a documented lawful use exists.

Schedule 3 - Country transfer schedules

3.1 Bahrain

For Bahrain-origin data, Customer will comply with Law No. 30 of 2018 and applicable decisions. The parties acknowledge that India is included in the current Bahrain Order 42/2022 adequate-country list for transfers without prior Authority authorisation under that Order. Customer remains responsible for other lawful-processing, notice/security and special-data requirements.

3.2 Oman

For Oman-origin Workforce data, Customer will obtain the data subject’s overseas-transfer consent where required by current Oman rules/guidance, complete the prescribed transfer risk/protection assessment, and obtain any required permit/approval before transferring sensitive data abroad. Bizmitra will provide the information reasonably necessary for that assessment.

If Oman employees were already active before this DPA/consent workflow, the parties will treat the rollout as remediation for continuing processing. No party will describe later consent as retroactively curing earlier processing. Customer will maintain a remediation record showing notice/consent rollout, completion status, transfer assessment and any sensitive-data findings.

Suggested Oman consent: “I understand that my employer uses Bizmitra Workforce, operated by Drushtant Infoweb Private Limited in India, for employment administration such as payslips and leave. I understand that the Workforce data made available by my employer will be stored and processed in Mumbai, India, outside Oman, and that Workforce data is not sent to OpenAI or Bizmitra’s German AI environment. I expressly consent to this overseas transfer and processing for those purposes. I may contact my employer about withdrawal and any alternative process available where the law permits.”

The consent must be separate from general Terms, affirmative/not pre-selected, and recorded with the exact version, date/time, employee identifier and language. Where valid consent must be freely given, Customer will provide a reasonable alternative way to receive a payslip/HR service if consent is refused.

3.3 United Arab Emirates

Customer will document the lawful processing basis and an international transfer mechanism permitted by UAE Federal Decree-Law 45/2021 and applicable implementing/sector rules. Contractual safeguards will be added where required. Customer will notify Bizmitra before uploading sector-regulated or localisation-restricted data.

3.4 Saudi Arabia - activation condition

Saudi production processing will not be activated until Customer and Bizmitra complete the applicable Saudi PDPL Article 29 / transfer-regulation analysis, transfer risk assessment and authorised safeguard such as SDAIA Standard Contractual Clauses where required, plus any sector-specific conditions.

3.5 Kuwait - activation condition

Kuwait production processing will not be activated until the parties confirm the applicability of CITRA Decision 26/2024 and any sector/localisation/approval requirements and document the lawful transfer/contract mechanism.

3.6 Qatar

Customer will comply with Qatar Law 13/2016, including applicable lawful-purpose/basis, notice/consent, security, rights and special-data permit requirements. Bizmitra will process on instructions and provide reasonable processor assistance.

3.7 Malawi

Customer will satisfy Malawi Data Protection Act 2024 requirements applicable to international processing/transfer and privacy information. Each party will assess any Data Protection Authority registration duty, including significant-importance thresholds applicable to its processing.

3.8 Bangladesh

Customer will classify its data and identify any Bangladesh localisation/cross-border requirement before upload. Data legally required to remain or be synchronously maintained in Bangladesh must not be placed in the standard Mumbai-hosted service unless an expressly compliant deployment is agreed.

3.9 Nepal

Customer will use Nepal personal data for the disclosed lawful purpose, obtain any required consent/authority and disclose India hosting as required. Bizmitra will process on documented instructions.

3.10 EEA / UK

Where GDPR/UK GDPR applies to a Customer transfer to Bizmitra in India and no adequacy mechanism is available, the parties incorporate the applicable EU Standard Contractual Clauses (controller-to-processor or processor-to-processor module as appropriate) and, for UK data, the UK Addendum/IDTA or another lawful mechanism. The Order Form/DPA processing details provide the annex information to the extent applicable; the parties will complete any additional fields required by the chosen mechanism.

Schedule 4 - Minimum technical and organisational measures

Control area	Measure
Access control	Role-based customer access; restricted administrative access; customer-managed authorised users and permissions.
Transport security	TLS-protected website/API traffic.
Tenant separation	Logical tenant scoping and application-level isolation controls.
Operations	Firewalling, monitoring, patching, logging and restricted production administration.
Backups	Automated infrastructure/database backup controls for the Mumbai ERP/Workforce environment.
Auditability	Security logs and application/financial audit controls appropriate to the Service.
Incident response	Triage, containment, investigation, recovery and customer notification/cooperation as required.

Control area	Measure
AI boundary	No current OpenAI/Germany processing of Workforce Customer Personal Data; limited forecast summary excludes identifying customer/employee details.

Schedule 5 - Signature / incorporation

This DPA is incorporated automatically when the governing customer agreement says so. If separately signed, the signature block below may be used.

For Bizmitra	For Customer
Drushtant Infoweb Private Limited Name: _____ Title: _____ Date: _____ Signature: _____	Legal name: _____ Name: _____ Title: _____ Date: _____ Signature: _____

© 2026 Bizmitra · Data Processing Addendum v2.0 · Generated Nov 5, 2026