Bizmitra

Regional Privacy Supplements

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

Jurisdiction-specific additions to the Privacy Notice for India, the GCC, Malawi, Bangladesh, Nepal and the EEA/UK.

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.

These Supplements form part of the Bizmitra Global Privacy Notice. They add jurisdiction-specific information and do not reduce any mandatory right. If a Supplement conflicts with a mandatory local rule, the mandatory rule prevails.

1. India

For processing governed by Indian law, Bizmitra applies the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 where applicable, and relevant CERT-In cybersecurity directions.

Where Bizmitra directly collects sensitive personal data or information within the scope of the 2011 Rules, we provide required privacy information, use the information for the disclosed purpose, apply reasonable security practices and handle disclosure/transfer in accordance with the applicable rule and contract.

CERT-In directions require covered entities to maintain ICT-system logs for a rolling 180-day period within India and to meet applicable incident reporting/cooperation requirements. Security-log retention may therefore differ from ordinary product-data retention.

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 are being brought into force in stages. This Supplement does not present provisions that have not yet commenced as current Data Principal rights or Bizmitra obligations. We will update this Supplement as relevant substantive provisions actually become operative.

India grievance contact: grievance@bizmitra.io.

2. GCC - general

There is no single GCC privacy law. Bahrain, Oman, UAE, Saudi Arabia, Kuwait and Qatar have separate legal frameworks. Where Bizmitra processes customer/employee data for a GCC organisation, the organisation remains responsible for its lawful basis, employee/customer notice and any permit/approval that only the local controller can obtain. Bizmitra provides the India-hosted processor service described in the DPA.

2.1 Bahrain

Bahrain processing is subject to Law No. 30 of 2018 and implementing decisions where applicable. India is included in Bahrain's current Order No. 42 of 2022 list of countries/territories to which a controller may transfer personal data without prior Authority authorisation under that Order. This does not remove the employer/controller's other notice, lawful-processing, security or special-data obligations.

For existing Workforce employees, the employer should provide the Workforce Privacy Notice and maintain evidence that the notice was delivered/acknowledged where appropriate.

2.2 Oman

Oman’s Personal Data Protection Law (Royal Decree 6/2022) and current MTCIT guidance apply where relevant. MTCIT currently states that, as a rule, the data subject’s consent is required before personal data is transferred abroad; non-sensitive overseas transfers also require the safeguards and risk/protection assessment contemplated by the Regulations. Sensitive categories identified by Oman law require additional permit/approval, and MTCIT states that sensitive personal data stored or processed outside Oman requires Cyber Defence Centre approval.

For Workforce data hosted in Mumbai, the Oman employer/controller must implement the separate overseas-transfer notice/consent and complete the transfer risk/protection assessment. Consent obtained after an existing deployment should be recorded as remediation for continuing processing and must not be represented as retroactively curing earlier processing.

Bizmitra’s standard current Workforce schema for the described Oman deployment does not collect fingerprint/face templates, health data or criminal/security information as dedicated Workforce fields. Device biometric unlock is performed locally by the employee’s phone and is not a transfer of the employee’s fingerprint/face template to Bizmitra.

Royal Decree 68/2026 amending the Oman Personal Data Protection Law was issued on 3 September 2026 and states that it takes effect on the day after publication in the Official Gazette. At this document cut-off, the operative amendment text had not yet been verified in the official Gazette; Bizmitra will review and update the Oman supplement when the operative text is available.

2.3 United Arab Emirates

Where Federal Decree-Law No. 45 of 2021 applies, the UAE customer/controller is responsible for its lawful processing basis and notices. International hosting in India must rely on a mechanism permitted by Articles 22-23 or other applicable UAE rules, including adequate protection or contractual/other permitted safeguards where required. Sector-specific localisation or regulator rules remain the customer’s responsibility unless expressly addressed in an Order Form.

2.4 Saudi Arabia

Saudi Personal Data Protection Law and the Regulation on Personal Data Transfer Outside the Kingdom apply where relevant. For a Saudi deployment, the controller must complete the applicable transfer assessment and use an authorised safeguard such as SDAIA Standard Contractual Clauses where required. Bizmitra will not activate the currently pending Saudi Workforce deployment until the applicable transfer requirements have been documented and agreed.

2.5 Kuwait

Kuwait CITRA Decision 26/2024 replaced the prior 42/2021 privacy regulation for the communications/IT regulatory context. Before activating the currently pending Kuwait Workforce deployment, the customer and Bizmitra will confirm whether the CITRA regulation, sector-specific rules, localisation requirements or approvals apply to that organisation/data and will document the required transfer/contract terms.

2.6 Qatar

Where Qatar Law No. 13 of 2016 on Personal Data Privacy Protection applies, the Qatar customer/controller is responsible for the lawful purpose/basis, required notices/consents, security and any special-data permits. Bizmitra processes customer-controlled data on instructions and assists with rights/security obligations under the DPA.

3. Malawi

Where Malawi’s Data Protection Act 2024 applies, the customer/controller is responsible for lawful processing, privacy information, data-subject rights and any requirements for international transfers to India. Bizmitra will provide processor safeguards under the DPA. Each party should assess registration if it becomes a controller or processor of significant importance; the Malawi Data Protection Authority has stated a current threshold that includes processing personal information of more than 10,000 Malawi-resident data subjects or processing of significance to Malawi’s economy, society or security.

4. Bangladesh

Bangladesh enacted the Personal Data Protection Act, 2026 and related national data-management legislation. A Bangladesh customer must identify any applicable data classification, localisation, synchronous-copy, regulator or cross-border requirement before uploading data to Bizmitra’s India-hosted service. Bizmitra will not represent the standard Mumbai deployment as satisfying a Bangladesh localisation requirement that requires data to remain in Bangladesh; a compliant alternative must be expressly agreed before such data is processed.

5. Nepal

Nepal’s Privacy Act 2075 (2018) and related rules protect personal information and confidentiality. Nepal customers must collect/use employee/customer information for a lawful disclosed purpose, obtain required consent/authority and disclose the India hosting where required. Bizmitra processes customer-controlled records under the DPA and supports verified rights requests.

6. EEA / United Kingdom where applicable

If the EU GDPR, UK GDPR or related data-protection law applies to a particular Bizmitra processing activity, Bizmitra will apply the rights and processor obligations required by that law. Where a customer exports EEA/UK personal data to Bizmitra in India and no adequacy mechanism applies, the parties will use the applicable EU Standard Contractual Clauses and/or UK transfer addendum/IDTA or another lawful transfer mechanism. OpenAI’s current DPA includes EU/UK transfer provisions for API processing where applicable.

The mere global availability of the Bizmitra website does not itself change the role allocation for customer-controlled data. A customer remains responsible for determining whether its own activities trigger GDPR/UK GDPR requirements and for providing required notices/lawful bases to its data subjects.

7. Regional rights and complaints

Local law may provide rights additional to the Global Privacy Notice and may permit complaints to the relevant regulator/authority. Where Bizmitra acts as processor, submit the request to the customer/employer controlling the record; Bizmitra will provide reasonable assistance. Where Bizmitra acts as controller, contact privacy@bizmitra.io.