

PRIVACY POLICY & DATA PROTECTION FRAMEWORK

Effective Date: July 30, 2026

Governing Regulation: Digital Personal Data Protection Act, 2023 (DPDP Act, India)

Data Protection Officer (DPO) Contact: dpo@brihos.com

Applicability: Applies globally to all information collected, stored, or processed via the Brihos Platform, its mobile applications, and software modules.

For purposes of this Policy:

“Personal Data”, “Data Fiduciary”, “Data Processor” and “Data Principal” shall have the meanings assigned to them under the Digital Personal Data Protection Act, 2023.

1. DUAL LEGAL ARCHITECTURE: DATA FIDUCIARY VS. DATA PROCESSOR

Brihos Data Privacy Ecosystem

The data privacy architecture under the DPDP Act, 2023, divides the platform's operations into two separate legal tracks:

- **Corporate B2B User Data (Brihos as a Data Fiduciary):** Brihos acts as a Data Fiduciary for corporate accounts. It directly determines the purposes and technical means of processing data for platform log-ins, account registration details, and corporate business parameters.
- **End-Consumer / Guest Data (Brihos as a Data Processor):** Brihos generally acts as a Data Processor in relation to Guest data processed on behalf of Accommodation Providers and Travel Agents, except where Brihos independently determines the purpose and means of processing.

1.1 Brihos as a Data Fiduciary

The Company acts as a Data Fiduciary when it determines the purposes and means of processing personal data. This capacity is limited strictly to:

- Account registration details, corporate parameters, and Know Your Customer (KYC) documentation provided by Accommodation Providers and Travel Agents.
- Interaction data, cookies, and system analytics captured when users navigate brihos.com or download official mobile applications.

1.2 Brihos as a Data Processor (The Enterprise Software Shield)

The Company generally acts as a Data Processor when providing its cloud-based Enterprise Software Suite (including the Hotel PMS, Banquet PMS, CRM engine and Direct Booking Engine), except where Brihos independently determines the purpose and means of processing personal data.

- **The Ultimate Fiduciary:** The Accommodation Provider or Travel Agent remains responsible for complying with applicable data protection obligations in relation to Guest data submitted through the Platform.
- **Notice and Consent Defensibility:** The Accommodation Provider remains responsible for complying with applicable notice, consent, retention and deletion obligations in relation to Guest data processed through the Platform.
- **Operational Scope:** Brihos merely processes, computes, and stores Guest data inside secure cloud infrastructure under the explicit technical instructions of the property.

2. METRIC COLLECTION & CATEGORIZATION OF DATA

2.1 B2B Account Datasets (Processed as Data Fiduciary)

- **Identity Metrics:** Full legal name of business owners, authorized corporate representatives, company registration proofs, Permanent Account Numbers (PAN), and Goods and Services Tax Identification Numbers (GSTINs).
- **Contact Information:** Official business mailing addresses, corporate email coordinates, telephone metrics, and verified mobile numbers.
- **System Telemetry:** Device information, browser settings and technical usage data.

2.2 End-Consumer/Guest Data (Generally Processed on Behalf of Accommodation Providers and Travel Agents)

- **Profile Records:** Full traveller names, age logs, gender information, residential addresses, contact parameters, and email coordinates.
- **Statutory Identification Data:** Scanned copies or numerical datasets of Government-issued identification documents uploaded by Users or Accommodation Providers where required under Applicable Laws.
- **Transactional Folio Data:** Check-in and check-out timestamps, banquet reservation parameters, dining configurations, room preference logs, and localized CRM history maps.

3. PRINCIPLES OF DATA PROCESSING: NOTICE, CONSENT, AND LEGITIMATE USES

3.1 Unambiguous Consent Architecture

To the extent that Brihos collects data as a Data Fiduciary, processing is built entirely upon clear, affirmative, itemized consent frameworks:

- **Clear Notice Requirement:** All data requests are preceded by an explicit digital privacy notice outlining the exact purpose of data capture, written in plain language.
- **Consent Management Dashboard:** Users may review, update or withdraw consent where such functionality is made available through the Platform.

3.2 Legitimate Uses Disclaimer

In accordance with the statutory provisions of the DPDP Act, Brihos or its licensed Accommodation Providers may process specific personal elements without explicit affirmative consent under conditions of Legitimate Use, encompassing:

- Responding to sudden medical emergencies, public health hazards, or natural disasters affecting a guest on property grounds;
- Complying with binding court orders, central law enforcement warrants, cyber-security mandates, or statutory income tax queries issued under Applicable Law.

4. CLOUD SOFTWARE PRIVACY CONSTRAINTS & INTERMEDIARY RULES

4.1 CRM Marketing Restrictions and Anti-Spam Bounds

- Accommodation Providers and Travel Agents are strictly prohibited from utilizing the Brihos CRM data engine to execute automated spam distributions, unsolicited marketing broadcasts, or continuous promotional text/email loops without possessing a verifiable, documented opt-in authorization from the targeted Guest.
- The Accommodation Provider or Travel Agent remains responsible for compliance with applicable marketing, privacy and consent requirements

and shall indemnify Brihos against claims arising from unauthorized marketing communications.

4.2 Automated AI Privacy Guardrails

- AI-powered features embedded within the Enterprise Software Suite may be used to generate recommendations, summaries, insights or operational suggestions. Brihos implements reasonable technical and organisational safeguards designed to protect personal data processed through such features.
- Brihos implements reasonable technical and organisational safeguards designed to prevent unauthorized disclosure of personal data through AI-enabled features.

4.3 Third-Party Distribution Integration Bridges

When an enterprise user connects the Platform to external distribution channels or global wholesalers (such as HotelBeds, RezLive, GRN, or connected Channel Managers), the personal data elements strictly necessary to finalize the reservation are transmitted via secure integration bridges. Upon exiting Brihos cloud parameters, the processing of that data shifts exclusively under the privacy policies and compliance liability parameters of the receiving external entity.

5. PRINCIPLE OF STORAGE LIMITATION & COMPLIANCE DATA BREACH MANAGEMENT

5.1 Retention and Erasure Limitations

- **Corporate Account Data:** Retained for the active duration of the underlying software subscription contract and for an additional period mandated by Indian tax and accounting statutes to satisfy auditing regulations.
- **Guest Software Data:** Data stored within the PMS or CRM containers is maintained in accordance with the instructions of the controlling Accommodation Provider or Travel Agent, subject to Applicable Laws and legitimate business, regulatory or security requirements. Upon formal cancellation of service or an explicit erasure payload instruction sent by the property, Brihos will execute irreversible deletion protocols across active database shards within thirty (30) days, unless prohibited by local policing laws.

5.2 Mandatory Breach Notification Mechanisms

In the event of any confirmed security compromise, technical system exploit, server disruption, or unauthorized access impacting personal data residing on the platform:

- **To the Property/Agent:** Brihos will notify the impacted Data Fiduciary without undue delay upon technical validation of the incident, providing relevant information reasonably necessary to enable damage assessment and mitigation, where required by Applicable Laws.
- **To the State Authorities:** In strict alignment with the DPDP Act, Brihos will file an explicit, formatted data compromise alert directly with the competent authority under the DPDP Act and all impacted corporate stakeholders within the legally prescribed timelines.

6. DATA PRINCIPAL RIGHTS & GRIEVANCE REDRESSAL

Every citizen whose personal data enters the platform holds explicit, enforceable statutory rights under the DPDP Act:

- **Right to Summary:** The right to request and view a clean, transparent breakdown of what personal data logs are currently stored on the platform and why they are being processed.
- **Right to Correction:** The right to instantly rectify, update, or complete broken, inaccurate, or outdated profiling and registration metrics.
- **Right to Erasure:** The right to request structural deletion of personal datasets across active database shards, invoking the statutory "Right to be Forgotten."
- **Right to Escalation:** The right to direct compliance grievances through an explicit portal path directly to the platform's Data Protection Officer (DPO), with further recourse to the competent authority under the DPDP Act.

7. COOKIES & SIMILAR TECHNOLOGIES

Brihos may use cookies, pixels, analytics tools and similar technologies to improve Platform functionality, security, user experience and performance.

8. CROSS BORDER TRANSFERS

Personal data may be processed or stored in locations outside the User's jurisdiction, subject to applicable legal safeguards and contractual protections.

9. SECURITY MEASURES

Brihos maintains reasonable technical, organisational and administrative safeguards designed to protect personal data against unauthorized access, loss, misuse, alteration or disclosure.

10. CHILDREN'S DATA

The Platform is not intended for individuals under eighteen (18) years of age. Brihos does not knowingly collect personal data from children except as required in connection with lawful hospitality bookings made by adults.

11. GRIEVANCE MECHANISM

Users may submit privacy requests, withdrawal of consent requests, correction requests or complaints to:

Data Protection Officer
Email: dpo@brihos.com

In the event of any inconsistency between this Privacy Policy and the Brihos Master Terms of Use, this Privacy Policy shall prevail with respect to the collection, use, processing, storage, transfer, protection and disclosure of personal data.