THE RESIDENCY GROUP OF HOTELS

Privacy Policy

How we collect, use, and protect personal data

Document	Privacy Policy
Applies to	Guests, employees, contractors, vendors, and website/app users
Owner	Data Protection Officer / IT Security & Compliance
Version	2.0
Effective date	14 August 2026

1. Purpose & Scope

This Privacy Policy sets out how The Residency Group of Hotels ("the Company," "we," "us") collects, uses, stores, shares, and protects personal data belonging to guests, employees, job applicants, contractors, and visitors to our properties and digital platforms. It reflects current data-protection practice, including the principles of India's Digital Personal Data Protection Act (DPDP Act, 2023) and, where applicable to international guests, comparable global standards such as the GDPR.

2. Definitions

- Personal Data — any information that identifies or can identify a natural person (name, contact details, ID/passport number, payment data, biometric or facial-recognition data captured at check-in, vehicle number, IP address, device identifiers).
- Sensitive Personal Data — government ID numbers, payment card data, health information (e.g. dietary/medical needs shared for a stay), biometric data, and children's data.
- Data Principal — the individual to whom the personal data relates (guest, employee, applicant, visitor).
- Data Fiduciary — the Company, which determines the purpose and means of processing personal data.
- Processing — any operation performed on personal data: collection, storage, use, sharing, or deletion.

3. What Data We Collect

Guest data

- Identity and contact details provided at booking or check-in (name, address, phone, email, government ID/passport as required by law).
- Payment and billing information, processed via PCI-DSS-compliant payment gateways.
- Stay history, preferences, and loyalty programme data.
- CCTV footage captured in public and back-of-house areas for safety and security.
- Wi-Fi and in-room technology usage logs, and website/app cookies and analytics (see the cookie notice on our booking site).
- Special requests such as dietary or accessibility needs, provided voluntarily by the guest.

Employee and applicant data

- Recruitment and employment records, payroll and statutory filings, access-card and system-login data, and performance records, handled under separate HR policies referenced from this document.

4. Legal Basis & Consent

- Data is processed on the basis of guest/employee consent, performance of a booking or employment contract, compliance with legal obligations (e.g. police/foreigner-registration rules, tax law), or legitimate business interest (e.g. property security).
- Consent for optional processing — marketing communications, loyalty profiling, non-essential cookies — is opt-in and can be withdrawn at any time without affecting service delivery.
- Where a Notice is required under applicable law, it will be provided in clear language at the point of collection, in English and the primary regional language of the property.

5. How We Use Personal Data

- To create and manage bookings, check-in/check-out, billing, and loyalty accounts.
- To meet legal and regulatory obligations, including statutory guest-registration requirements.
- To maintain the safety and security of guests, staff, and property (including CCTV monitoring).
- To personalise service and, with consent, to send offers and promotional communications.
- To manage employment relationships and internal IT systems.

Data is not used for any purpose incompatible with the purpose for which it was collected, in line with the Company's data-minimisation principle.

6. Sharing of Personal Data

Personal data is shared only where necessary — with payment processors, booking/OTA platforms, cloud and IT service providers, government authorities where legally required, and other Group properties for a confirmed stay. All external sharing is governed by the Third-Party Policy and, where applicable, a signed Data Processing Agreement. We do not sell personal data.

7. Security Measures

- Role-based access control and multi-factor authentication for systems holding personal data.
- Encryption of data in transit and at rest for reservation, payment, and HR systems.
- Regular vulnerability assessment, patching, and independent security review of cloud and on-premise infrastructure.
- Documented incident-response procedure with breach notification to affected individuals and the relevant regulator within the timelines required by law.

8. Your Rights

Guests and employees have rights to access, correct, and request erasure of their personal data, and to withdraw consent, subject to legal retention requirements. These rights, and how to exercise them, are set out in full in the Guest Rights Policy (for guests) and the internal HR Data Handbook (for employees).

9. International Data Transfer

Where personal data is transferred outside India (for example, to a cloud hosting region or an international OTA partner), the Company ensures an appropriate transfer mechanism — such as standard contractual clauses or an equivalent safeguard — is in place, consistent with DPDP Act requirements.

10. Contact & Grievance Redressal

Questions, complaints, or requests relating to this Policy may be directed to the Data Protection Officer at the property's front office or via the contact details published on the Company website and on in-room guest directories. Complaints are acknowledged within 2 business days and resolved within 30 days.

11. Policy Review

This Policy is reviewed at least annually, and whenever there is a material change in law, technology, or business practice, by the Information Security & Data Protection Committee under the authority of the Approving Authority.

This policy is confidential and intended solely for internal use, authorized guests, and contracted third parties as applicable. It is reviewed annually by the Information Security & Data Protection Committee.