THE RESIDENCY GROUP OF HOTELS

Third-Party Policy

Standards for vendors, partners, and service providers handling our data

Document	Third-Party Policy
Applies to	Vendors, contractors, OTAs, payment processors, cloud/IT providers, and business partners
Owner	IT Security & Compliance, with Procurement and Legal
Version	2.0
Effective date	14 August 2026

1. Purpose & Scope

This policy governs how The Residency Group of Hotels engages third parties who access, process, or store Company or guest data — including Online Travel Agencies (OTAs), payment gateways, cloud hosting and SaaS providers, marketing and CRM vendors, facility contractors, and IT support partners. It sets the minimum security, privacy, and contractual requirements that apply before, during, and after any such engagement.

2. Categories of Third Parties

- Technology & cloud providers — hosting, PMS (property management system), backup, and SaaS applications.
- Distribution partners — OTAs, global distribution systems, and travel agents who receive booking and guest-contact data.
- Payment processors — PCI-DSS-certified gateways and card networks.
- Marketing & CRM vendors — email/SMS platforms, loyalty programme providers, analytics providers.
- Operational contractors — housekeeping, security, maintenance, and facility-management vendors with premises or system access.

3. Due Diligence Before Engagement

- Every new vendor with access to Company systems or guest/employee data undergoes a security and privacy risk assessment before onboarding.
- Higher-risk vendors (those processing sensitive personal data, payment data, or with system-level access) require evidence of a recognised certification (e.g. ISO 27001, PCI-DSS, SOC 2) or an equivalent security review.
- Procurement maintains a register of all active third parties with data access, reviewed at least annually.

4. Contractual Requirements

- A written Data Processing Agreement (or equivalent confidentiality and security clause) is required before any personal data is shared, specifying purpose, data categories, security obligations, and retention/deletion terms.
- Contracts must prohibit the vendor from using Company or guest data for any purpose beyond the agreed service, and from selling or further disclosing it without written consent.
- Vendors must notify the Company of a security incident or data breach involving Company/guest data within 24 hours of discovery.
- Sub-processors engaged by a vendor (e.g. a cloud sub-host) must be disclosed and approved before use, and are bound by equivalent obligations.

5. Minimum Necessary Data Sharing

- Only the data required for the vendor to perform the contracted service is shared — never a full guest or employee database by default.
- Shared data is transmitted through approved, encrypted channels (secure file transfer, API with authentication, or an access-controlled shared folder) — never unprotected email or public shared drives.
- Access granted to a third party is role-based, logged, and reviewed at the end of the engagement or at least annually for ongoing relationships.

6. Security Expectations for Third Parties

- Encryption of Company/guest data in transit and at rest.
- Multi-factor authentication for any remote or system access granted to vendor personnel.
- Timely patching and vulnerability management on any system that touches Company data.
- Background-verified personnel for on-site contractors with data or premises access.

7. Monitoring & Audit

The Company reserves the right to request evidence of compliance, conduct security questionnaires, or — for critical vendors — commission an independent audit. Non-compliance identified during monitoring triggers a remediation plan with a defined timeline; unresolved critical issues can lead to suspension of data access.

8. Termination & Data Return

- On termination of a vendor relationship, all Company and guest data held by the vendor is returned or securely destroyed within 30 days, with written confirmation.
- System and premises access for the vendor is revoked on the effective date of termination.
- Retention exceptions apply only where the vendor has an independent legal obligation to retain specific records.

9. Non-Compliance

Failure by a third party to meet the requirements of this policy is treated as a material breach of contract and may result in suspension of access, termination of the engagement, and, where the breach involves personal data, notification to affected individuals and regulators in line with the Privacy Policy.

10. Ownership & Review

This policy is owned by IT Security & Compliance in coordination with Procurement and Legal, and is reviewed annually or upon any material change in the Company's vendor landscape or applicable law.