THE RESIDENCY GROUP OF HOTELS

Data Retention Policy

How long we keep data, and how it is securely disposed of

Document	Data Retention Policy
Applies to	All personal, financial, operational, and IT data held by the Company
Owner	IT Security & Compliance, in consultation with Finance and HR
Version	2.0
Effective date	14 August 2026

1. Purpose & Scope

This policy defines how long The Residency Group of Hotels retains different categories of data, and how data is securely disposed of once it is no longer required. It applies to physical records, IT systems, backups, and data held by third parties on the Company's behalf, and reflects the data-minimisation and storage-limitation principles of current data-protection practice.

2. Retention Principles

- Data is kept only as long as necessary for the purpose it was collected, a legal/statutory obligation, or a legitimate business need.
- Retention periods below are minimum/maximum guidance; the longer of a legal requirement or a stated business need applies.
- Data subject to an active legal hold, audit, or dispute is retained until that matter is resolved, regardless of the schedule below.
- Backups follow the same retention limits as the live data they contain, except where a shorter technical backup cycle applies.

3. Retention Schedule

Data category	Retention period	Basis
Guest registration / statutory ID records	As prescribed by local police/foreigner-registration regulation (typically 1–2 years)	Legal obligation
Reservation & billing records	8 years	Tax and financial-audit law
Payment card data	Not stored beyond transaction authorisation; tokenised where retained	PCI-DSS
Guest loyalty & preference profiles	Duration of active membership + 3 years, or until consent withdrawn	Consent / legitimate interest
Marketing consent & communication records	Until consent is withdrawn, then 1 year proof-of-consent record	Consent
CCTV footage	30–90 days, unless subject to an incident investigation	Legitimate interest / security
Employee HR & payroll records	Duration of employment + 7 years	Labour and tax law
Recruitment / applicant records (unsuccessful)	1 year	Legitimate interest
IT system logs & access logs	12 months	Security monitoring
Email & shared-drive business records	3 years, unless flagged for longer retention	Business need
Backup copies of the above	Mirrors source retention period; deleted from backup media on the same cycle	Business continuity

4. Secure Disposal

- Physical documents containing personal or confidential data are shredded on-site; general waste bins are never used.
- Electronic records are deleted using secure-erase methods; end-of-life hardware (drives, laptops, POS terminals) is wiped or destroyed by an approved ITAD vendor with a certificate of destruction.
- Cloud-hosted data is deleted (not merely archived) from production and backup systems once the retention period lapses, in line with the vendor's data-deletion SLA.
- Disposal of any dataset is logged, including date, method, and approver.

5. Legal Holds

Where the Company receives notice of litigation, regulatory inquiry, or a police request, the IT Security & Compliance team places a legal hold on the relevant data, suspending scheduled deletion until Legal confirms the hold is lifted.

6. Roles & Responsibilities

- Data Protection Officer — owns this policy and approves exceptions.
- IT Team — implements automated retention/deletion rules on core systems and backups, and executes secure disposal of hardware.
- Department Heads (Front Office, Finance, HR, Sales & Marketing) — ensure records specific to their function follow the schedule above.
- Employees — must not retain personal data in personal folders, devices, or unauthorised cloud storage beyond the periods above.

7. Review

This schedule is reviewed annually and updated immediately upon any change in applicable law (including DPDP Act rules, tax law, or labour law) or hotel-industry regulation.