DATA RETENTION POLICY

(As adopted by the Board of Directors on 23.05.2024)

TAJ GVK HOTELS AND RESORTS LIMITED (TAJGVK)

Contents

1. Introduction

This Data Retention policy has been adopted by TAJGVK in order to set out the principles for retaining, reviewing and destroying data. This policy covers all employees and all directors and officers of the TAJGVK, where ever they may be located or working. We also expect our consultants and third-party vendors to introduce and follow appropriate data retention practices.

2. Purpose

A Retention policy is required as TAJGVK to handle sensitive, personal and confidential data assets. This data must be collected, processed, stored and destroyed in a manner that makes business and economic sense and complies with legal requirements and contractual obligations.
This policy applies to all employees (including contractors) who process data (including personal information) held on computer systems or manual records within TAJGVK control or possession.

3. Applicability

This policy applies to all TAJGVK personnel and operating units.

4. Importance of data retention to TAJGVK

• TAJGVK needs to retain data for business, commercial and legal reasons and as part of good governance. However, retaining data for longer than is required for our business purposes or to meet legal obligations is neither necessary, nor advisable and in some cases (such as the excessive retention of personal information) may be unlawful.

• Excessive document and data retention is costly, and exposes TAJGVK to risk, such as:
  - The risk of breach of laws that require that personal information is only retained for as long as necessary for the business purpose for which it was collected and processed;
  - Data security breaches may be unnecessarily compounded, because the more data we hold the higher the risk of a breach to the business and the affected individuals; and
  - Discovery and disclosure exercises in the context of audits, litigation proceedings and/or regulatory investigations may become more labour intensive and costly than they need.

• Therefore, when there is no longer a legitimate business purpose to keep data, it should be deleted, except if a legal requirement to retain it for longer applies. Retaining data just in case it may be needed in future is not a legitimate business reason to keep data.

5. Responsibility for data retention

• The protection, retention and disposal of data is the responsibility of every TAJGVK employees and contractors, as well as third party employees, such as the employees of our service providers who store data on our behalf. It is therefore important that you have read and understood this policy. All employees and contractors of TAJGVK are obliged to adhere to this policy at all times.

• When dealing with a third party that handles personal data on TAJGVK's behalf, arrangements must be made to ensure that that third party handles such data properly. Such arrangements will typically involve a review of the third party's internal processes and imposing on the third-party appropriate obligations in a written agreement with TAJGVK. Such obligations must extend to data retention and deletion.

6. Data retention period

• Personal information (i.e., information that relates to identifiable individuals) can be lawfully retained only for as long as retention is necessary to achieve the legitimate business purpose for which the data is collected and processed. Ensuring compliance with this requirement means that TAJGVK and its employees must proactively manage personal information retention periods.

• Beyond personal information, TAJGVK has business requirements to retain other information, such as confidential information that is required for the normal conduct of our hospitality business or for accounting, tax or legal reasons.

• In some cases, such as in connection to accounting, tax or actual or potential litigation, TAJGVK is required to retain data, including personal information, for specified periods of time.

• In summary, where the law mandates retention and/or prescribes specific retention periods for specific types of data, the obligation to retain the data will prevail over the limitations concerning the retention of personal information.

• For example, even after an employee has left the organization, TAJGVK may need to keep information about the ex-employee to provide references or to defend legal claims like the employees PF details. However, if there is no objective reason that justifies keeping personal information, such data should be deleted or anonymized. The business process owner who is responsible for collecting the data is also responsible for ensuring that the data is anonymized or deleted in accordance with this policy.

7. Queries

For more information on data retention or any aspect of this policy, please contact your Unit IT Team who will help direct / answer your queries.

8. Policy review

This policy may be updated from time to time by TAJGVK to reflect any change in legislation or in TAJGVK's methods or practices.

9. Enforcement

• Breach of any of the principles within the policy may result in disciplinary action, and a serious breach–such as if an employee or contractor is found to be in wanton abuse of the policy and their

actions cause reputational risk or damage and/or financial loss to the business – may amount to gross misconduct, which may result in summary dismissal and contract cessation.

• This Policy is not intended to, and does not grant, users any contractual rights.

10. Data Retention Schedule

• Retention periods generally are counted from the date the underlying matter ceases to be active.

For example:

- A contract would be held for the specified period after its expiration or termination;
- A tribunal/court record would be retained for the specified period after the conclusion of the case;
- Guest records would be retained for the specified period after expiry of the customer relationship; and
- Employee records would be held for the specified period after the termination of the employment relationship.

• If a particular record is in two categories, the longer retention period applies.

Data retention schedule for TAJGVK: -

Record Type category	Retention Period	Reasons
Book of Accounts	6 years	
Payroll and salary records	7 years	
Employee tax records	8 years	
Reports on employee performance review meetings and assessment interviews (e.g., evaluations, employment application forms of successful applicants, copies of academic and other training received, employment contracts and their amendments, correspondence concerning appointment, appraisals, promotions and demotions, agreements concerning activities in relation to the works council, references and sick leave records)	3 years or 1 year after audit, whichever is later	
HR data like Provident fund information of employees	7 years	
CCTV	3 years	
Emails	5 years	Archive after 1 year
Subject Access Requests	5 years	
Electronic marketing data –	5 years	

customers		
Booking data, check-in data, special requests data	For as long as the guest remains a customer	
Financial data and credit card information	For as long as it is necessary to process the transaction, including any queries which may arise.	
Loyalty scheme information	For as long as the guest is an active participant in the loyalty scheme.	
Contact information of guest.	As long as the guest remains a customer.	
Health data special requests, or in connection with gyms or spas	1 years	
Information provided via tour operators and other 3rd parties. (Guest lists etc.).	7 years	
Guest details of current registration number, details of driving licence, details of passport (physical/electronic)	7 years	
System logs	18 months	