Privacy by Design Policy

Table of Contents

1. Purpose 2
2. Definition 2
3. Privacy by Design – General Principles 3
4. Technical and Organisational Measures 3
5. Privacy by Default 4
6. Data Protection by Design 4
7. Roles and Responsibilities 5
8. Compliance and Enforcement 5
9. Exception 5
10. Monitoring and Reporting 5
Appendix 6

1. Purpose

This policy is for employees, workers, and contractors of the Indian Hotels Company Limited (hereafter referred to as "IHCL" or "us" or "we"). When processing personal data (defined below), IHCL obliges to implement appropriate technical and organisational measures (taking into consideration the nature of the processing, risks to individuals and costs etc), into such processing activities in order to meet the requirements of the data privacy laws and protect the rights of the data subjects concerned. The 'appropriate measures' may change from one processing activity to the other, and it is important that such measures are given consideration at the start of, and throughout, the life-cycle of IHCL's processing of personal data. This obligation is referred to as 'Privacy by Design'. As a minimum, such measures must ensure that only personal data which are necessary for each specific purpose of the processing are processed and that the personal data is not made available to an indefinite number of individuals without the data subject's consent.

This Policy provides guidance on IHCL's approach to ensuring that it embeds privacy by design across IHCL's operations. Since 'Privacy by Deign' is a vital requirement of the data privacy laws, it is important that all staff understand and implement this Policy.
If you have any questions, please contact IHCL's Infosec team at dpo@tajhotels.com

2. Definition

Term	Definition
Personal Data	Means any information relating to an identified or identifiable natural person ('data subject')
Special Category of Personal Data	Means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. For the purpose of this policy, when we are referring to 'personal data', we are referring to Personal Data and Special Categories of Personal Data collectively.
Data Protection Impact Assessment (DPIA)	An assessment of the impact of the processing operations on the protection of personal data as referred to under Art 35 of GDPR;
Processing Principles	Means the processing principles set out in Art 5 of GDPR and as attached as an Appendix to this Policy.

3. Privacy by Design – General Principles

The principles of 'Privacy by Design' can be summarised as:

#	Principle
1	Use proactive rather than reactive measures. Anticipate, identify, and prevent privacy invasive events before they happen.
2	Privacy should be the default position. Personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy.
3	Privacy must be embedded and integrated into the design of systems and business practices.
4	All legitimate interests and objectives are accommodated in a positive-sum manner. Both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
5	Security should be end-to-end throughout the entire lifecycle of the data. Data should be securely retained as needed and destroyed when no longer needed.
6	Visibility and transparency are maintained. Stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.
7	Respect user privacy by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user-friendly options.

4. Technical and Organisational Measures

IHCL's aim is to implement appropriate technical and organisational measures which are designed:

(a) to implement the Data Protection Principles in an effective manner, and

(b) to integrate into the processing of personal data the safeguards necessary for that purpose.

This Policy applies at the time of determining the means of processing, and at the time of actually processing the personal data.

In doing so, IHCL will consider the available technical and organisational measures, the cost of implementation and the nature, scope, context and purposes of processing of personal data, as well as the risks of varying likelihood and severity for rights and freedoms of individuals presented by the processing of their personal data.

If it is considered that the processing presents a high risk to individuals, a DPIA must be carried out in accordance with IHCL's data privacy policy.

5. Privacy by Default

IHCL's aim is that appropriate technical and organisational measures will be applied to ensure that, by default, only the personal data which is necessary for each specific purpose of processing of personal data is used, in relation to:

(a) the amount of personal data collected;
(b) the extent of processing that personal data;
(c) the period of its storage; and
(d) its accessibility.

IHCL's aim is that by default personal data should be restricted to those who have a business need to know.

6. Data Protection by Design

IHCL's aim is that when considering a proposal for a particular type of processing of personal data, the impact of this on the individuals affected should be considered, and that appropriate technical and organisational measures should be put into place to ensure that:

(a) the Data Protection Principles are implemented; and

(b) any risks to individuals' rights and freedoms are minimised.

Vigilance by staff should be exercised continually to ensure the security of IHCL systems and personal data, e.g., against attempts to trick individuals into revealing their log-in details; and to avoid risks of personal data breaches arising from mobile devices and remote log-ins. Staff should avoid downloading, working with, or storing identifiable personal data wherever possible, and only undertake these activities in compliance with appropriate guidance and policies. Anonymised or partly/reversibly anonymised data should be used wherever possible.

When buying systems/software which involve personal data or considering transfers/sharing of personal data including using the "cloud", staff must evaluate the privacy and security of alternative solutions and vendors/partners. The use of such systems/software should to the maximum extent possible avoid personal data being involved or put at risk of a data breach. Personal data should only be placed on systems, devices or software where this is compliant with IHCL's policies and the applicable legislation. The use, and duration of holding, of personal data should be minimised. Reviews of, and improvements to, privacy should be undertaken regularly by staff in their areas of work, documented, and privacy risks and precautions reviewed by staff regularly.

Managers or staff should not purchase new systems or software without first reviewing their proposed use in terms of a Data Protection Impact Assessment if the proposed use presents a high risk to individuals, and the proposed purchase also requires to be checked first by Procurement and by Information Services for contract terms, and for the uses of, and risks to, personal data. For purchasing supplies/services, regardless of contract value, no managers or staff should approve a contract with a supplier unless the terms have been checked for data protection compliance.

7. Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Ensuring overall compliance with the present policy • Ensuring each new initiatives follows the requirements defined in this policy • Providing support for risk assessment, recommendations, and Implementation of appropriate controls • Involved in the contract defining and reviewing process
IHCL IT team	• Developing the DPIA based on the availability requirements • Implementation of necessary security measure to comply with the security requirements defined in the present policy

8. Compliance and Enforcement

Periodic audits of compliance shall be conducted at least annually. Results shall be documented, and any deficiencies corrected.

9. Exception

Any exception to this policy must be documented and forwarded to the Chief Information Security Officer CISO for review and approbation, which needs to be vetted by CIO also.

10. Monitoring and Reporting

This document shall be reviewed once a year or at the time of any major change in existing environment affecting policy, whichever is earlier.

This document contains controlled copies of the procedure listed above. Any copies made from this document, in part or in whole, are uncontrolled and are therefore not subject to further review, revision or approval.

Appendix

Article 5: Principles relating to processing of personal data:

1.Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken toensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).