MINOR
INTERNATIONAL

PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

This Personal Data Protection Policy ("**Privacy Policy**" or "**Policy**") sets out how Minor International PCL and its affiliates (referred to as "**we**", "**our**", "**us**" or "**the Company**") handles the Personal Data of our customers, suppliers, employees, consultants and other third parties.

By collecting and using Personal Data, we are subject to a variety of legislation that sets how such activities may be carried out and the safeguards that must be put in place to protect it. The purpose of this Policy is to inform all employees about the steps that must be followed to ensure compliance with all applicable privacy regulations.

This Privacy Policy together with Related Policies and Privacy Guidelines are forming a data protection framework that will govern the Company's employee's conduct regarding Personal Data collection, use, storage, and destruction of the data, as well as any specific rights the data subjects may have.

2. SCOPE

This Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy is mandatory and applies to all employees. Any breach of this Privacy Policy will result in disciplinary action. All employees need to implement appropriate practices, processes, controls, and training to ensure compliance.

We share this responsibility with our consultants, contractors, advisors, and vendors ("**Third-Party Recipients**"). We have an obligation to ensure that Third-Party Recipients adhere to the same level of Personal Data protection as us, and that is why every Third-Party Recipient must sign the Data Processing Agreements before they begin processing Personal Data.

3. PRINCIPLES

We adhere to the generally recognized principles relating to the processing of Personal Data which include:

Lawfulness: personal data is to be processed lawfully, fairly, and in a transparent manner. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. We should be transparent and honest with people when we collect their personal data.

Transparency: The laws require us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through an appropriate Privacy Statement which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Data Minimization: The personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed. The Company shall ensure any Personal Data collected is adequate and relevant for the intended purposes and when Personal Data is no longer needed for specified purposes, it shall be deleted or anonymised in accordance with the Company's data retention guidelines.

Accuracy: Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. The Company will ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Employees must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

Storage Limitation: Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. Employees must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Company's applicable Personal Data Retention Policy. This includes requiring Third-Party Recipients to delete Personal Data where applicable.

Security, Integrity, and Confidentiality: Personal Data must be secured by appropriate technical and organizational measures against unauthorized or unlawful Processing and against accidental loss, destruction, or damage. Employees must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction and may only transfer Personal Data to Third-Party Recipients who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

4. DATA SUBJECTS RIGHTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold, provided that such access does not violate our confidentiality obligations;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests;
- object to decisions based solely on Automated Processing, including profiling (Automated Decision-Making aka ADM);
- be notified of a Personal Data Breach which is likely to result in a high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used, and machine-readable format.

These data subject rights are not absolute and are subject to our other obligations such as protection of the information that belongs to other individuals. We must verify the identity of an individual requesting data under any of the rights listed above and comply with the company's Data Subject Request Policy.

5. PERSONAL DATA BREACH

In the event of a Personal Data Breach, based on the magnitude of the breach, we must notify the relevant regulators and the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any relevant regulator where we are legally required to do so. Please consult the Breach Management Policy for more information and reach out to Personal Data Protection Office if you have any questions.

6. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure

compliance with data privacy principles. We must also conduct Data Protection Impact Assessment with respect to high-risk Processing activities or when implementing major system or business change programs.

7. SHARING PERSONAL DATA

We are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. Employees may only share the Personal Data we hold with another employee, agent, or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

Employees may only share the Personal Data we hold with Third-Party Recipients if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a Data Processing Agreement has been signed.

8. DATA PROTECTION OFFICE

If you have any questions about Personal Data processing, please contact the relevant section of the data protection office:

1. Asia, Africa and Middle East

Email: privacy.corporate@minor.com; or

Post: 88 The Parq Building, 12th Fl. Ratchadaphisek Road, Klongtoey Subdistrict, Klongtoey District, Bangkok Metropolis 10110, Thailand

2. Europe and America

Email: dpo@nh-hotels.com; or

Post: Calle Santa Engracia 120, 7ª, 28003, Madrid

3. Australia

Email: Privacy.corporate@minorhotels.com.au; or

Post: PO Box 473, Cotton Tree, QLD 4558, Australia

9. AUDIT

The Company is committed to maintaining a robust data protection program and ensuring compliance with this Policy and applicable data protection laws. Regular audits and assessments shall be conducted to monitor and evaluate the effectiveness of data protection measures.

In the event of a suspected or actual Personal Data Breach, the Company shall promptly initiate an investigation to assess the severity and impact of the breach. Appropriate remedial actions shall be taken to mitigate any potential harm to individuals and to prevent future breaches.

10. DISCIPLINARY ACTION

The Company maintains a zero-tolerance policy regarding Personal Data Breaches and non-compliance with this policy or applicable data protection laws. Any employee, contractor, or third party found to have violated this policy may be subject to disciplinary actions, which may include but are not limited to:

(a) Verbal or written warnings.
(b) Additional training on data protection and privacy.
(c) Temporary suspension or revocation of access to personal data.
(d) Termination of employment or contractual agreements.

The severity of the breach and the level of non-compliance shall be considered when determining the appropriate disciplinary actions. The Company shall ensure that any disciplinary actions taken are fair, consistent, and in accordance with applicable employment or contractual laws.

Employees and contractors are encouraged to report any suspected or actual breaches of this Policy or data protection laws to the data protection office. Whistleblower protection measures shall be implemented to protect individuals who report breaches in good faith.

11. TRAINING AND AWARENESS

The Company recognizes the importance of providing adequate training and promoting awareness among employees, contractors, and third parties regarding data protection and privacy.

Regular training programs shall be conducted to ensure that individuals involved in the collection, processing, or management of personal data are aware of their responsibilities, understand the requirements of this policy, and are knowledgeable about relevant data protection laws.

Ongoing awareness initiatives, such as communication campaigns, posters, and internal newsletters, shall be implemented to reinforce data protection principles and best practices throughout the organization.

12. RELATED DOCUMENTS

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Mapping Procedure
- Legitimate Interest Assessment Template
- Data Retention Policy
- Data Protection Executive Committee Terms of Reference
- Breach Management Policy
- Data Subject Request Policy
- Information & Consent Procedure

13. POLICY OWNERSHIP AND MAINTENANCE

The owner of this Policy is Data Protection Executive Committee who is also responsible for its maintenance and accuracy. This Policy and all the related documents are available to all the Employees through the Data Privacy SharePoint.

Changes to this Policy will come into force when published on the Data Privacy SharePoint. Notice of significant revisions will be provided to all Employees by the Data Protection Team.

All enquiries, requests for exceptions or changes must be directed to the Data Protection team via e-mail privacy.corporate@minor.com.

Appendix I: Glossary

Term:	**Definition:**
Automated decision-making (ADM)	Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Automated decision-making often involves profiling, but it does not have to.

Consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data Controller	The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Subject	An identified or identifiable natural person.
DPIA	Data Protection Impact Assessment
Personal Data	Any information relating to an identified or identifiable living natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier (as determined by the applicable laws and regulations), including but not limited to name, date of birth, photograph, video footage, email addresses, telephone numbers, an identification number, financial information, location data, and online identifiers.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processing	Any operation (or set of) which is performed on personal data.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a person.
Third-Party Recipients	consultants, contractors, advisors, or vendors, who are authorized to process Personal Data.