DESTINATION ASIA

DESTINATION MANAGEMENT FOR ASIA'S TRAVEL CONNOISSEURS

Data Privacy at Destination Asia

Destination Asia is committed to ensuring that all of our activities (and in particular those that concern personal data) meet or exceed the compliance standards of the jurisdictions in which we conduct our business. We place great importance on our customers', employees', suppliers' and business contacts' privacy and the security of their personal data. We are determined to maintain operations which treat individuals' privacy with respect, fairness, transparency and integrity honouring the trust they place in us by sharing their data with us.

The global nature of our business means that we must comply with data privacy laws and regulations not only in countries where we have an office, but in all countries to which we market, and from where we collect personal data.

We understand you have questions about how we handle personal data. We hope the below information is helpful to you. If you require further information, please reach out to us at privacy@destination-asia.com.

Sincerely,
Destination Asia Data Privacy Office

DESTINATION ASIA

DESTINATION MANAGEMENT FOR ASIA'S TRAVEL CONNOISSEURS

Our Commitment

We commit to having appropriate policies and procedures designed to protect the privacy and security of personal data. Below we describe our key commitments.

Data Privacy Officer and Data Privacy Office

We have appointed a Data Privacy Officer who is supported by a Data Privacy Office made up of representatives from our IT, cybersecurity, legal and audit departments. The Data Privacy Office defines and maintains various policies and procedures and evaluates compliance with those policies and procedures across our organisation.

Privacy Principles

We follow seven core privacy principles which our employees and contract workers must also follow in their day-to-day activities. Our privacy principles are:

- **Lawfulness, fairness, transparency:** We process personal data based on an appropriate legal basis and do this fairly and transparently to individuals;
- **Purpose Limitation:** We process personal data only for a specified and legitimate purpose and no further;
- **Data Minimisation:** We ensure that the personal data we process is adequate, relevant and is not more than required for the purpose;
- **Storage Limitation:** We ensure that personal data is not kept for longer than is necessary for the purpose;
- **Accuracy:** We ensure that the personal data is accurate and kept up to date;
- **Security:** We ensure that appropriate technical and organisational measures are in place to prevent unauthorised or unlawful processing, loss, destruction or damage to the personal data;
- **Accountability:** We maintain records to demonstrate compliance with these privacy principles.

Privacy by Design and Privacy by Default

We consider our privacy principles up front when we start a new project; develop or design new services, products or systems; and use third party applications, services or products, which involve personal data. We also take into account the rights of individuals and design our projects, services, products and systems to be able to meet those rights. Our policies and procedures are designed to ensure that, by default, only personal data which is necessary for a specific purpose of processing is processed.

Privacy Impact Assessments and Data Processing Agreements

We conduct privacy impact assessments to assess privacy and security risks where our projects, services, products and systems involve personal data might result in high risk to the rights and freedoms of individuals. As a global organisation, we need to transfer personal data around the world. When we share personal data with others or we engage with other parties who process personal data on our behalf, we strive to adopt the highest standards of personal data protection, including by having appropriate data processing and data transfer agreements in place.

Awareness and Confidentiality

We ensure that our employees are properly trained and have a continuous awareness of personal data privacy and security. Our employees must adhere to a privacy policy that mirrors our organisational commitments. Besides having a privacy policy in place, we ensure that the employment contracts we conclude with new employees joining our organisation have proper confidentiality clauses.

Data Retention

We have policies in place that are designed to ensure that personal data is not kept for longer than is necessary based on organisational and legal needs.

Data Breach Incident Response

We have technical controls in place designed to prevent data breaches, but in the event a data breach occurs, we have an incident response plan in place to mitigate the risks of a data breach and to notify regulators and individuals as appropriate.

Data Subjects' Rights

We are committed to being transparent with individuals about how their personal data is processed through our Privacy Notice. We also have processes in place which are designed to fulfil the rights individuals have under applicable law, such as the right to access copies of personal data and the right to object to processing personal data.

Information Security Measures

We have cyber security controls in place to prevent unauthorised processing, loss, destruction or damage of personal data. Our cybersecurity department, in cooperation with the Data Privacy Office, implements security measures to a level appropriate to the risk of processing personal data. Access to information and to our IT assets is provided only on a "need to know" and "least access" basis.

We are committed to the safety and security of our IT systems, therefore we have security technologies, processes and defined responsibilities in place to deal with ongoing vulnerabilities and threats. Where we consider it necessary, the storage and transmission of data is secured by using appropriate means, such as encryption, masking or fudging.