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

Introduction

Destination Asia is required to comply with the applicable data privacy laws and regulations in respect of its processing of personal data (such as information about our customers, employees, and suppliers). Our objective is to set out the data privacy principles which we will apply to our processing of personal data so that we not only respect the data privacy rights of individuals and process their personal data in accordance with the law, but also safeguard of our most valuable assets, data.

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. This Policy is designed to ensure compliance with applicable EU data privacy laws, such as the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and such standard should ensure compliance in the majority of the jurisdictions in which we operate. Where further measures are needed in particular jurisdictions, the Data Privacy Office will advise impacted stakeholders separately.

Your Responsibilities

All employees and contract workers ("Employees"), must familiarise themselves with this Policy (as well as any other data privacy related policies, procedures and/or processes that may be applicable to your area of work) and comply with them whenever you process personal data. Failure to do so may expose Destination Asia to fines and enforcement action taken against it by data protection supervisory authorities, which could result in restrictions being imposed upon Destination Asia which prevent us from exploiting personal data commercially and/or to complaints and claims for compensation from affected individuals. There may also be negative publicity as a result of our non-compliance.

Any failure to comply with this Policy will be taken seriously, dealt with promptly and may result in disciplinary measures which could ultimately result in dismissal.

Data We Process

Destination Asia processes personal data about a range of Living Persons, such as employees, customers, suppliers and business contacts, and the personal data concerned may be in any form, including but not limited to electronic data, paper documents and disks and all types of processing, whether manual or automated that is under Destination Asia possession or control.

We process personal data for a number of purposes, such as customer administration, marketing, profiling our customers and suppliers, statistical analysis, credit checking, service delivery, employee administration, payroll and employee medical and insurance. It is critical to our business that we are able to use personal data in this way. In order to continue to be able to do so, we must ensure compliance with the principles set out in applicable data privacy laws and regulations and in this Policy.

Definitions

In order to fully appreciate the principles in this Policy it is important for you to understand the meaning of certain key words and phrases. These are set out below:

- **Data controller** - is the organisation that determines the purposes for which and the manner in which personal data is processed. For example, Destination Asia is the data controller. Employees are not data controllers.

- **Data processor** - is an organisation appointed by the data controller to process personal data on its behalf. Destination Asia appoints external organisations to process personal data on our behalf, on the basis that they follow our instructions and do not make decisions in respect of the processing for their own purposes. Examples of these might include a supplier who provides

transfer service, our IT outsourced services provider or our customer data analytics provider. On the other way round, Destination Asia can also be a data processor for MICE clients.

- **Informed Consent** - is any given specific and informed indication of the Living Person's agreement to the processing of his/her personal data.

- **Living Person** - is a living identified, or identifiable individual, about whom we process personal data. An identifiable individual is someone who can be identified, directly or indirectly, for example, a person could be identifiable by a name, an identification number, location data or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Under data protection laws and regulations the term 'Data Subject' is used to described a Living Person. However, for ease of reference we have used the term Living Person in this Policy.

- **Personal data** - is any information capable of identifying a Living Person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link.

- **Personal data breach** - is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Processing** - any operation (or set of operations) that is performed upon personal data, whether or not by automatic means, including, but not limited to collection, recording, organisation, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction (and process, processes and processed is interpreted accordingly).

- **Sensitive personal data** – certain types of personal data are considered to be "sensitive" and additional care needs to be taken when handling such data.

    - The following personal data is defined by law as sensitive: health; racial or ethnic origin; religious or philosophical opinions; trade union membership; political opinions; sexual life or sexual orientation; genetic or biometric data (for the purpose of uniquely identifying a living individual); criminal history/ criminal convictions.

    - Additionally, to what is defined by law, Destination Asia may require certain other categories of data to be handled with special care.

References in this Policy to 'we' and 'our' refer to Destination Asia and 'you' refers to Employees.

Our Commitment

We commit to having appropriate policies and procedures designed to protect the privacy and security of personal data. Below we describe our 7-key commitments.

7 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:

1. **Lawfulness, fairness, transparency:** We process personal data based on an appropriate legal basis and do this fairly and transparently to individuals;

1.1 All processing of personal data must be justified by reference to one of a number of "conditions" for processing. If you cannot find a condition that justifies your processing then the processing may not take place. However, in the majority of cases, processing will be justified on the basis that:

- it is in Destination Asia's legitimate interests as a business or employer, except where such interests are overridden by the interests or fundamental rights and freedoms of Living Persons;
- we have obtained the Living Person's consent to the processing (this is not normally appropriate for Employees);
- it is necessary to perform a contract. For example, where customer has booked a holiday with us and we process their personal data in order to organise and deliver their holiday; or
- it is necessary to comply with a legal obligation to which Destination Asia is subject (other than an obligation imposed by contract).

1.2 Sensitive personal data should only be processed where it is absolutely necessary to do so. Additional consideration should be given to the secure storage and transmission of sensitive personal data, and access rights should be strictly limited. In addition, where you are processing data which is classified as sensitive personal data by law, one of the following conditions must be satisfied:

- the explicit consent (e.g. by actively ticking a box or making a clear written or oral statement) of the Living Person has been obtained, except where consent is precluded under applicable laws;
- the processing is necessary for an obligation of Destination Asia under employment law;
- the vital interests of the Living Person need to be protected (e.g. in a medical emergency or other life or death situation); or
- the processing is necessary for the purpose of legal proceedings or obtaining legal advice.

1.3 If you are considering implementing a new project or way of working or making changes to an existing project or way of working, which will involve the processing of personal data, it is important to consider (and record) the condition which can be relied upon together with the rationale for the processing. Destination Asia maintains a Personal Data Inventory which records certain details about all business processes which use personal data. The Personal Data Inventory may need to be updated to reflect the new or revised project or way of working.

1.4 In addition, in such situations, consideration should be given to whether a Data Privacy Impact Assessment should be carried out. Please refer to data privacy impact assessments and when they should be carried out.

1.5 The second requirement of the first principle is that personal data must be processed fairly. This means that the way in which personal data is held and used must be kept consistent with the privacy notice provided to the Living Person. We satisfy this requirement in relation to our customers, for example, by informing them in a customer privacy policy, which is made generally available on our

website(s), how their personal data is used, (amongst other things) about the types of personal data collected, the purposes for which the personal data are collected, anyone to whom their personal data may be disclosed outside of Destination Asia and the rights available to them.

1.6 The customer privacy policy must be given to the Living Person at the right time. Where we obtain personal data directly from the Living Person (e.g. as a result of a telephone call or online collection) we must give the customer privacy policy to the Living Person at the time we obtain his data.

1.7 The customer privacy policy must be prominent, in legible font and included at every point where we collect personal data, such as in application forms, websites, call centre scripts, promotion terms and application terms. If, for example, the customer privacy policy is provided online, it must be accessible behind a prominent hypertext link where appropriate in the online journey.

1.8 In certain circumstances, short form privacy notices may be presented to Living Persons and included on data collection forms, internet portals etc., in each case these should include a link to the applicable full privacy policy.

2. **Purpose Limitation:** We process personal data only for a specified and legitimate purpose and no further;

2.1 personal data must be obtained only for one or more specified and lawful purposes. Our customer privacy policies will specify the purposes for which we will process personal data and we are not permitted to process those data for a new purpose, without first considering the need to obtain Informed Consent from the Living Person and/or issuing an updated privacy notice; and

2.2 personal data must not be further processed in any manner incompatible with the purpose(s) for which the data were originally obtained. A breach of this principle could also result in a breach of the first principle. For example, if a customer privacy policy describes the purposes for which personal data will be used as administration, marketing and risk assessment, we should not use those data for any other purposes, unless those additional purposes would be totally obvious to the individual. To do otherwise could result in unfair processing in breach of the first principle and a breach of the second principle.

3. **Data Minimisation:** We ensure that the personal data we process is adequate, relevant and is not more than required for the purpose;

3.1 you identify the personal data needed for a particular purpose and you collect the minimum amount required to properly fulfil that purpose. Care must be taken to avoid collecting excessive or irrelevant elements of personal data;

3.2 you do not hold personal data on a 'just-in-case' basis because you think it might be useful in the future but without having any clear idea of what that future purpose might be;

3.3 you keep personal data up to date (otherwise personal data which were originally adequate may cease to be so); and

3.4 you do not keep personal data for longer than the purposes for which it was originally collected unless there is a clear overriding business need or legal/regulatory requirement (otherwise that data may cease to be relevant and become excessive).

4. **Storage Limitation:** We ensure that personal data is not kept for longer than is necessary for the purpose;

Personal data must not be retained for longer than the purpose(s) for which it was originally collected unless there is a clear overriding business need or legal/regulatory requirement to retain the personal data. You should review the personal data which you hold on a regular basis and delete any data which is no longer required in connection with the purpose for which it were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data. Destination Asia's Data Retention Policy sets out the procedures for ensuring that documents/records are updated, archived and deleted appropriately as well as suggested timeframes for the retention of key categories of documents/records.

5. **Accuracy:** We ensure that the personal data is accurate and kept up to date;

5.1 Personal data will be inaccurate if it is incorrect or misleading as to any matter of fact (e.g. an incorrect name or address). If you are inputting data onto our system and are unsure as to the accuracy of certain information (e.g. because you cannot read the handwriting or because it looks like an obvious mistake or omission), in the first instance speak to your line manager for guidance about how you can verify the accuracy of the information.

5.2 We will not be in breach of this principle, even if we are holding inaccurate personal data, if:

- we accurately recorded those data when we received them from the Living Person or a third party, and
- we took reasonable steps to ensure the accuracy of those personal data, and
- if the Living Person has notified us that the personal data are inaccurate, we have taken steps to indicate this fact (e.g. by making a note that we have received an objection).

5.3 You must take reasonable steps to keep personal data up to date to the extent necessary. The purpose for which personal data is held will determine whether it needs to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated.

6. **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;

6.1 All Employees have a responsibility to help keep personal data secure. As set out in section 6.2 below, Employees should, in particular, be aware of the obligations and follow the recommendations in the Information Assets Security Policy and the Information Assets Acceptable Use Policy Further, all Employees who have access to personal data are under a legal responsibility to keep information confidential.

6.2 This sixth data privacy principle requires Destination Asia to take appropriate technical and organisational measures to protect the personal data which we process:

- technical measures include: software controls to restrict user access; up-to-date virus checking software; audit trail software; encryption, all of which we manage through IT Security.
- organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; training Employees on the care and handling of personal data; all of which you are responsible for complying with and applying to your daily routine.

6.3 Where personal data is transmitted outside of Destination Asia, for example to a third party service provider who may need to process personal data on our behalf, a secure medium must be used to transmit such data and a written agreement (containing the required level of security standards and data protection obligations) should be in place with each such third party prior to any disclosure of personal data to that third party. In all such instances, please ensure that you comply with our Third Party Data Sharing Process. In addition, consideration should also be given as to whether a data privacy impact assessment should be carried out.

7. **Accountability:** We maintain records to demonstrate compliance with these privacy principles. This seventh data privacy principle requires us to demonstrate that we comply with all the above-mentioned data privacy principles and requirements and it is our responsibility to do so. We achieve this by various different methods, including:

- implementing appropriate technical and organisational measures, such internal and external facing policies, procedures, processes, records and notices, that meet data privacy principles/requirements and comply with all applicable data privacy laws;
- using data privacy impact assessments, where appropriate; and
- accurately documenting our processing activities.

Data Privacy Requirements

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.

The Data Privacy Office is responsible for determining when a data privacy impact assessment is required, for completing certain parts of the assessment and for signing-off on its findings. However, the responsibility for identifying a project which may be in scope for an assessment rests with the business, and with the owner of that project.

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.

Consequences of Non-Compliance and Accountability

If we are found to be in breach of applicable data privacy laws and regulations, data privacy supervisory authorities may impose monetary penalties, or issue other enforcement proceedings against us which could result in our being prevented from further use of the affected personal data, or being required to change our processing procedures, or having other conditions imposed upon us in respect of the processing of personal data. Enforcement action will usually have a cost and time implication for the business. However, more damaging might be any restrictions imposed upon us which prevent us from exploiting our databases commercially.

Additionally, the associated publicity could make us appear as an organisation that does not respect the privacy rights of individuals and cause us reputational damage.

Affected Living Persons may also take legal action against us and claim compensation for any breaches of applicable data privacy laws and regulations on our part that have resulted in damage (or damage and distress) to the Living Person.

Periodic monitoring of adherence to this Policy takes place to help ensure compliance with this Policy, applicable data protection laws and/or contractual agreements in connection with the handling of personal data. As set out earlier in this Policy, it is the responsibility of all Employees to assist Destination Asia to comply with this Policy. It is therefore key that all Employees familiarise themselves with both this Policy and apply their provisions in relation to all processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal.

Policy Ownership and Responsibility

The owner of this Policy is the Data Privacy Office., The Data Privacy Office shall ensure that this Policy is properly applied at Destination Asia and is responsible for the oversight and implementation of this Policy. The Data Privacy Office is responsible for communicating Policy requirements and any revisions made to this Policy.

Policy Review Cycle

This Policy shall be reviewed periodically to ensure that the Policy is meeting all of its objectives. Changes to applicable data protection laws, regulation or regulatory regimes may form triggers for revisions or updates to this Policy. It is the responsibility of all Employees to assist Destination Asia to comply with this Policy.

Queries and Waiver

The Data Privacy Office is available to help give constructive advice on this Policy in consultation with Destination Asia Legal who will advise on legal issues. Any instances where a waiver of this Policy is sought must first be reported to the Data Privacy Office.

Updated - March 2022