GDPR Compliance Statement

Corporate Traveller takes pride in protecting the personal data that we hold or process about our clients, employees, vendors and other stakeholders. Corporate Traveller is committed to best practice in complying with data protection requirements across our entire global operation.

Corporate Traveller has embraced the General Data Protection Regulation ("GDPR") as a baseline standard for its operations globally. Similar to existing legal requirements, compliance with the GDPR requires a partnership between Corporate Traveller and our corporate customers in their use of our services.

As a data controller, Corporate Traveller applies its Data Processing Addendum ("DPA") when providing travel services, enabling clients to transfer data to Corporate Traveller with confidence. Corporate Traveller's DPA describes the roles and responsibilities of Corporate Traveller and our clients, the scope of data processing, cooperation and assistance requirements, data security, transfer mechanisms and the technical and organisational measures used in the delivery of our services.

Our Global Approach

The broad scope of the GDPR means it can impact businesses outside of Europe. As a global brand, Corporate Traveller has implemented an integrated global programme to ensure a robust and consistent approach to data protection compliance across our entire network. In addition we have appointed global and regional data protection officers to establish an ongoing focus on data security.

GDPR Compliance Statement

Our commitment to protecting personal information

Corporate Traveller's Data Protection Officer can be contacted at data.protection@corptraveller.co.uk

Collection of Data

Our policy is to collect only the personal data necessary for agreed purposes and we ask our clients to only share personal data where it is strictly needed for those purposes.

Corporate Traveller consultants only use traveller's personal data for the purpose for which it was collected, which generally involves the fulfilment of travel bookings and other travel-related services.

To provide global travel services Corporate Traveller needs to process traveller data. As the data controller, Corporate Traveller provides travellers all necessary notices and information via our websites and booking tools.

Guiding Principles

- **Accountability:** we take responsibility for our obligations and are accountable to our stakeholders.
- **Trust:** We collect, store, share and use personal data in a responsible and ethical manner.
- **Compliance:** We achieve sustainable compliance with our legal obligations to protect personal data and support and encourage the proper handling and use of all other data held by the Corporate Traveller network, including confidential information.
- **Consistency:** We have a uniform and coordinated approach to data protection across our business.
- **Security:** We leverage our technical and organisational measures ("TOMs") to protect data. Such TOMs are set out in our in our DPA accessible by visiting corptraveller.co.uk/trust-and-compliance
- **Transparency:** We are clear and open with all key stakeholders about how we handle, use and protect data.

ICO Registration

Corporate Traveller is registered with the UK supervisory authority. Our registration can be seen on the Information Commissioner's ("ICO") website under reference Z7994553.

Security

Corporate Traveller has always taken the privacy and confidentiality of your employees' personal data seriously. We comply with our obligations under all applicable privacy and data protection laws, in all the jurisdictions where we operate.

Our Data Security Standards are set out in our DPA, the full details of which can be accessed via the trust and compliance page on www.corptraveller.co.uk and which cover:

1. Data Security Governance
2. Physical Access Control
3. Virtual Access Control
4. Data Access Control
5. Disclosure Control
6. Data Entry Control
7. Instructional Control
8. Availability Control
9. Separation Control

GDPR Compliance Statement

Our commitment to protecting personal information

Record of Processing

As part of Corporate Traveller's global GDPR programme, records of processing activity are produced and maintained.

Data Protection Impact Assessments

Procedures are in place to flag processing activities that might represent a high risk to the rights and freedoms of data subjects so that data protection impact assessments ("DPIAs") are carried out. When risks are identified, mitigating actions are identified, implemented and recorded.

Transparency

All applications and IT systems display the appropriate privacy notices for users. Where consent is used for marketing purposes, the consent is accurately recorded and managed in our system. See additional section below on 'Marketing and Communication Consent'.

Information Management

Policies and data retention schedules are maintained to ensure that personal (as well as other) data are kept no longer than is necessary and to prevent its use beyond its original intended purpose.

Data Protection by Design and Default

Corporate Traveller's IT function has developed and applied guidance and training in data protection by design and default. This enables us to make sure that new systems or applications have data protection measures built in up-front.

Information Security Incident Management

Corporate Traveller has robust incident response capabilities in order to deal effectively with issues arising from a data breach. Our response procedures are regularly reviewed and tested to ensure they operate effectively and are aligned with the GDPR requirements.

Business Continuity

Corporate Traveller has a robust business continuity plan in place.

Our role as Controller

When we process client employees' personal data to make and manage travel arrangements on their behalf we do so as a controller. We only process client employee personal data for this purpose and under the contract with the client.

Suppliers / Subcontractors and Other Third Parties

Appropriate due diligence is always performed prior to appointing any external service provider who will be processing personal data. Risk and information security is included within comprehensive contractual agreements that include explicit content to cover availability, confidentiality and compliance with necessary legal and regulatory requirements.

Agreements / contracts with subcontractors have, at a minimum, equivalent obligations as those required in our contracts with our clients.

GDPR Compliance Statement

Our commitment to protecting personal information

Corporate Traveller uses a number of third party processors to provide certain elements of our IT systems and the support for them. We and our third party service processors have host servers and data centres throughout the world. Corporate Traveller puts in place contractual arrangements with such processors which comply with Corporate Traveller's strict standards of security and confidentiality. We will only transfer personal data outside the European Economic Area ("EEA") to a third party processor who (i) is in a country which provides an adequate level of protection for personal data or (ii) is under an agreement with us which covers the EU requirements for the transfer of personal data to data processors outside the EEA.

Where personal data are processed on behalf of Corporate Traveller by a data processor, such processing will be carried out in accordance with Corporate Traveller's instructions/ contractual terms which provide for the return, destruction or deletion of personal data in certain circumstances such as termination or expiry of the contract.

We regularly review our contractual provisions with suppliers and third parties to make sure that they adequately cover the standards required under GDPR.

Marketing and General Communication

Corporate Traveller believes it is important to provide our clients with information about us and our range of services as well as insights into travel management, thought leadership and industry updates and advisory articles. Through our client relationship management system, we issue regular communications on a subscription basis.

Contact with 'Corporate Subscribers' is conducted in accordance with an 'opted-in' status and is based on the principle of legitimate interests. With every communication, individuals are offered an opportunity to unsubscribe to receiving further email communication.

Behaviours and Culture

Corporate Traveller has a comprehensive change management, communications and training workstream which is constantly establishing improved cultural norms, values, beliefs and behaviours that relate to data protection at Corporate Traveller, including a mindset of data protection by design and default.

All Corporate Traveller staff are required to undertake mandatory annual Data Protection and Information Security courses, and all staff employment contracts detail employees' responsibilities in relation to confidentiality and privacy. Corporate Traveller takes appropriate measures to safeguard the integrity and confidentiality of data from unauthorised access.