POPIA Compliance Statement

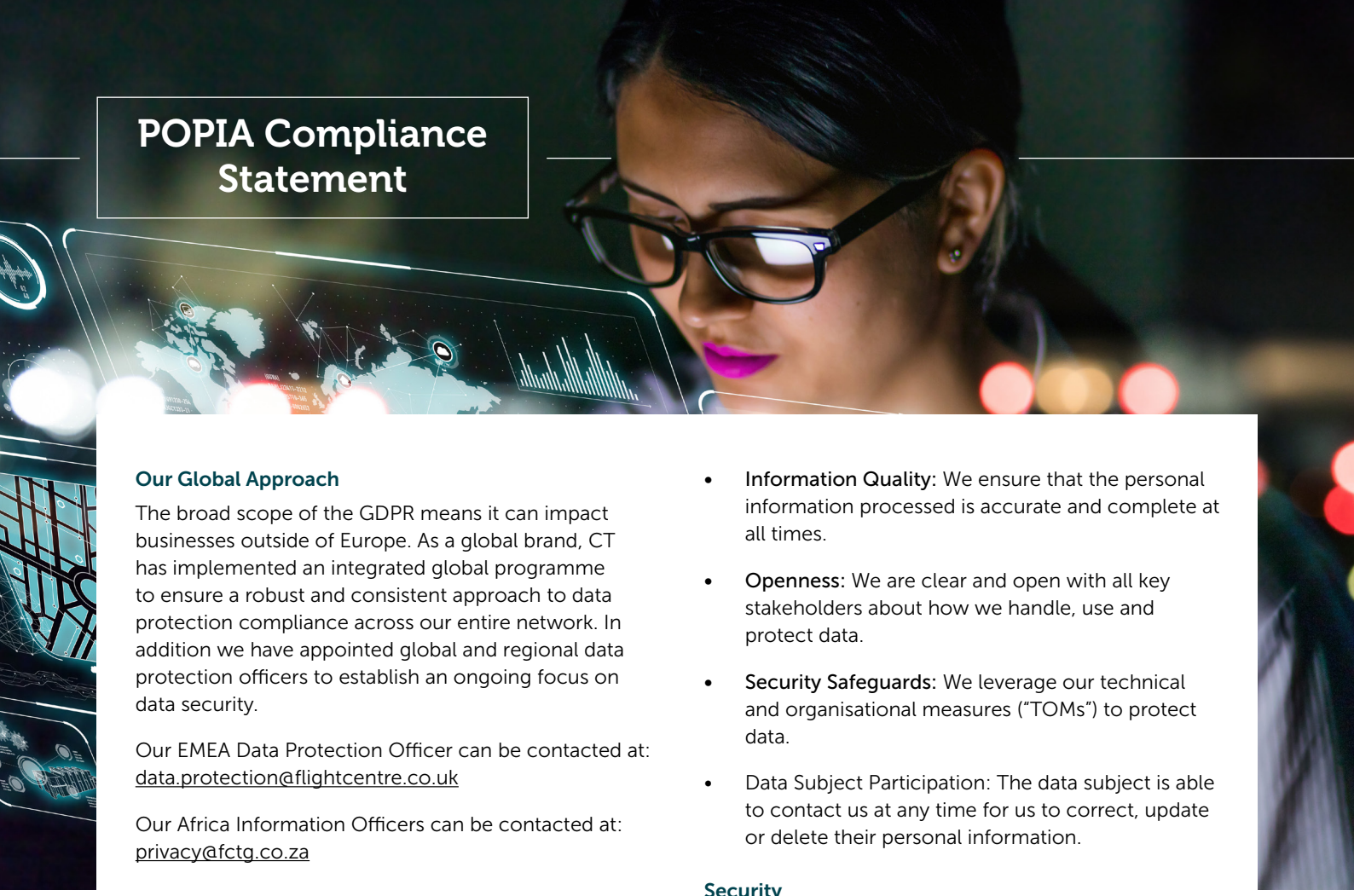
CORPORATE TRAVELLER™

bring an expert on board

Corporate Traveller, a division of FCTG Corporate (Pty) Ltd ("CT") takes pride in protecting the personal information that we hold or process about our clients, employees, vendors and other stakeholders. CT is committed to best practice in complying with data protection requirements across our entire global operation.

CT has embraced the General Data Protection Regulation ("GDPR") as a baseline standard for its operations globally. Similar to existing legal requirements, compliance with the Protection of Personal Information Act 4 of 2013 ("POPIA") requires a partnership between CT and our corporate customers in their use of our services.

As a responsible party, CT applies its Data Privacy Annexure ("DPA") when providing travel services, enabling clients to transfer data to CT with confidence. CT's DPA describes the roles and responsibilities of CT 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.



POPIA Compliance Statement

Our Global Approach

The broad scope of the GDPR means it can impact businesses outside of Europe. As a global brand, CT 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.

Our EMEA Data Protection Officer can be contacted at: data.protection@flightcentre.co.uk

Our Africa Information Officers can be contacted at: privacy@fctg.co.za

Collection of Data

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

CT consultants only use traveller's personal information 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 CT needs to process traveller data. As the responsible party, CT 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.
- **Processing Limitation:** We collect, store, share and use personal information in a responsible, ethical manner and for legitimate purposes.
- **Purpose specification:** Our customers are made aware as to why we need to process their personal information via our contractual relationship, whitepapers and privacy policy.
- **Further processing limitation:** In the event that personal information is processed again, it is used for the original intended purpose.
- **Information Quality:** We ensure that the personal information processed is accurate and complete at all times.
- **Openness:** We are clear and open with all key stakeholders about how we handle, use and protect data.
- **Security Safeguards:** We leverage our technical and organisational measures ("TOMs") to protect data.
- Data Subject Participation: The data subject is able to contact us at any time for us to correct, update or delete their personal information.

Security

CT has always treated the privacy and confidentiality of your employees' personal information with the utmost seriousness. We comply with our obligations under all applicable privacy and data protection laws, in all the jurisdictions where we operate.

CT is PCI-DSS certified. In markets where we do not hold this accreditation, we apply a global policy for data access, sharing, retention and deletion. CT adheres to the local and international data protection laws applicable to each region in which we operate.

Record of Processing

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

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 General Communication'.

Information Management

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

POPIA Compliance Statement

Data Protection by Design and Default

CT'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

CT 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 POPIA requirements.

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

Business Continuity

CT has a robust business continuity plan in place.

Our role as a responsible party

When we process client employees' personal information to make and manage travel arrangements on their behalf we do so as a responsible party. We only process client employee personal information 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 information. 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.

CT uses a number of third party operators to provide certain elements of our IT systems and the support for them. We and our third party service operators have host servers and data centres throughout the world.

CT puts in place contractual arrangements with such operators which comply with CT'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) where appropriate safeguards are in place authorise the transfer of personal data under GDPR.

Where personal data are processed on behalf of CT by a data processor, such processing will be carried out in accordance with CT's instructions/ contractual terms which provide for the return, destruction or deletion of personal information 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 POPIA.

Marketing and General Communication

CT 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

CT has a comprehensive change management, communications and training work stream which is constantly establishing improved cultural norms, values, beliefs and behaviours that relate to data protection at CT, including a mind-set of data protection by design and default.

All CT staff employment contracts detail employees' responsibilities in relation to confidentiality. CT takes appropriate measures to safeguard the integrity and confidentiality of data from unauthorised access.