DATA PRIVACY

1. **Definitions**

The terms defined in this Data Privacy Annexure shall be read as having the meanings set forth in (i) this Data Privacy Annexure and (ii) elsewhere in the Agreement. If a term is defined both in this Data Privacy Annexure and elsewhere in the Agreement then, for purposes of this Data Privacy Annexure, the definition in this Data Privacy Annexure shall prevail.

In this Data Privacy Annexure, references to any Applicable Privacy Laws and to terms defined therein shall be replaced with or incorporate (as the case may be) references to any Applicable Privacy Laws replacing, amending, extending, re-enacting, or consolidating such Applicable Privacy Laws and the equivalent terms defined in such Applicable Privacy Laws once in force and applicable.

1.1 "**Applicable Privacy Laws**" means all applicable data protection and privacy laws applicable to the Processing of the Customer Personal Information, including, when and where applicable, (a) POPIA; (b) EU General Data Protection Regulation EU 2016/679; (c) Electronic Communications and Transactions Act 25 of 2002 and (d) similar laws enacted anywhere in the world addressing the protection or the use, transmission, or other processing of Personal Information, each as amended, modified, and/or supplemented by the guidance or regulatory decisions of any relevant supervisory authority or other data protection regulatory authority ("**Regulator**").

1.2 "**Data Subject**" means any natural person about whom Personal Information relates.

1.3 "**Data Subject Request**" means any request by a Data Subject in respect of Personal Information Processed by a Responsible Party pursuant to the provision of the Services or otherwise in connection with the Agreement.

1.4 "**Good Industry Practice**" means the exercise of that degree of skill, diligence, prudence, and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking under the same or similar circumstances.

1.5 **"Operator"** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

1.6 "**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person), or as that term (or similar variants, such as "personal data") may otherwise be defined in Applicable Privacy Laws).

1.7 "**Personal Information Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Customer Personal Information in CT's possession or control. Personal Information Breaches include, but are not limited to: (i) unauthorised access, disclosure, loss, download, theft, blocking, encryption or deletion by malware or other unauthorised action in relation to the Customer Personal Information by unauthorised third parties; (ii) operational incidents which have an impact on the Processing of the Customer Personal Information; or (iii) any breach of this Data Privacy Annexure or Applicable Privacy Laws by CT, its employees or agents, to the extent that such breach affects the integrity and security of the Customer Personal Information or materially adversely impacts CT's obligations under this Data Privacy Annexure.

1.8 **"POPIA"** means the South Africa Protection of Personal Information Act (Act No. 4 of 2013), as implemented into national law and as amended, extended, re-enacted or applied by or under any other statute, law or enactment.

1.9 "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, restriction, degradation, erasure or destruction of information. Any activity defined as processing by or otherwise subject to the requirements of Applicable Privacy Laws shall fall within this definition. "Processed", "Process" and any other variations of "Processing" shall also be defined as set out above.

1.10 **"Responsible Party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for Processing Personal Information.

1.11 **"Customer Personal Information"** means Personal Information provided to CT by the Customer, its affiliates, employees, officers, contractors, representatives, agency workers, or end users to CT pursuant to the provision of the Services or otherwise in connection with the Agreement.

1.12 "**Supervisory Authority**" means any data protection authority or other governmental, regulatory, administrative, judicial, or other agency or similar body that has authority to implement, enforce, and/or oversee compliance with Applicable Privacy Laws.

1.13 "**Vendor**" means the transport, accommodation and other wholesale service providers such as airlines, coach, rail and car rental operators who CT engages on the Customer's behalf to deliver travel related products and services to the Customer.

2. **Parties as Responsible Parties and compliance with Applicable Privacy Laws.** The parties acknowledge that, in order to provide the Services, CT must necessarily process the Customer's Personal Information as a Responsible Party. Each Party shall act as a separate and independent Responsible Parties in relation to all the Customer's Personal Information it Processes under and/or in connection with this Agreement and the Services. Each party shall comply with all Applicable Privacy Laws in respect of its Processing of the Customer's Personal Information and shall ensure that it has a lawful basis for all such Processing, where applicable.

Where an affiliate of a party is a Responsible Party or Operator of the Customer's Personal Information under this Agreement, such party shall ensure that its affiliate complies with its obligations under the Applicable Privacy Laws and this Data Privacy Annexure as applicable.

3. **Information provided to Data Subjects.** Prior to sharing any Customer Personal Information with CT, the Customer shall provide all notifications required by Applicable Privacy Laws to the relevant Data Subject in each case with respect to the sharing of the Customer's Personal Information with CT. Where CT collects the Customer's Personal Information directly from Data Subjects, CT shall be responsible for ensuring that it provides clear and transparent information to Data Subjects, as required under Applicable Privacy Laws, in relation to the relevant Processing.

4. **Cooperation and assistance**. Each Party shall provide the other Party with such reasonable cooperation, assistance and information to the other to assist that other Party with its compliance with Applicable Privacy Laws.

5. **Notifications.** Each Party shall promptly notify the other (to the extent permitted by law) in writing providing reasonable detail of any third party complaint, audit, investigation or enquiry (whether by a Supervisory Authority, Data Subject or otherwise) establishing, alleging or enquiring as to possible non- compliance with any Applicable Privacy Laws in connection with the Customer Personal Information maintained by or for such Party, and the Parties will co-operate reasonably with each other in respect thereof.

6. **Personal Information Breaches.** The Parties are aware that Applicable Privacy Laws may impose a duty on a Party to inform a Supervisory Authority and the Data Subject in the event of Personal Information Breach affecting the Customer's Personal Information. In addition to complying with its notification requirements under Applicable Privacy Laws, CT shall promptly notify the Customer of any technical, organisational or other incidents (including incidents at Operators) which have resulted in a Personal Information Breach in the sense of Section 22(1) POPIA affecting the Customer's Personal Information. CT's notification of a Personal Information Breach to the Customer must be comprehensive and include any information required under Section 22(5) POPIA and/or required by Applicable Privacy Laws, as and to the extent such information is available.

   In the event of a Personal Information Breach, CT shall promptly take any measures required and appropriate under Applicable Privacy Laws and technical standards to restore the confidentiality, integrity and availability of the Customer Personal Information and the resilience of CT's processing systems and services and to mitigate the risk of harm and/or any detrimental consequences for the Data Subjects affected or potentially affected by the Personal Information Breach.

7. **Data Subject Requests.** Each Party will provide the other Party with reasonable assistance in complying with any Data Subject Request.

8. **Security.** In accordance with Good Industry Practice and Applicable Privacy Laws, each Party shall implement appropriate technical and organisational security measures (including maintaining any security controls) to ensure a level of security for Personal Information in such Party's possession or control that is appropriate to the risk presented by the Processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Customer Personal Information transmitted, stored or otherwise Processed.

   Without prejudice to the generality of the foregoing, the minimum technical and organisational security measures that CT shall implement and maintain are set out in the Schedule to this Data Privacy Annexure. CT may, from time to time, implement adequate alternative technical and organisational measures provided, however, that such measures shall not materially fall short of the level of security set out herein.

9. **Requirements as to personnel.** CT shall ensure that all personnel involved in the Processing of the Customer Personal Information are properly qualified and trained and have committed themselves to keep the Customer's Personal Information confidential or are under an appropriate statutory obligation of confidentiality in accordance with Applicable Privacy Laws.

10. **Appointment of data privacy personnel.** Where required, each Party will appoint authorised data privacy and security contact personnel.

11. **Appointment of Operators.** As a Responsible Party, CT maintains the right to appoint third-party Operators. If CT engages a third-party Operator to process the Customer's Personal Information for the purpose of providing the Services, CT shall agree to written terms with the Operator that: (i) require the Operator only to process the Customer's Personal Information for the purpose of delivering the Services; (ii) require the Operator to implement appropriate technical and organisational security measures to protect the Customer Personal Information against a Personal Information Breach; and (iii) otherwise comply with the requirements of Applicable Privacy Laws. CT shall remain responsible to the Customer for any breach of this Data Privacy Annexure that is caused by an act, error or omission of the Operator.

    Notwithstanding the above, Customer acknowledges that the Vendors to whom CT discloses Customer Personal Information in order to provide the Services are independent Responsible Parties under Applicable Privacy Laws, and not Operators. As such, the requirements concerning Operators described in the preceding paragraph do not apply to CT's disclosure of the Customer's Personal Information to Vendors.

12. **Transborder information flows.** In order to enable the efficient and effective delivery of its Services, CT may from time to time transfer and Process the Customer Personal Information from South Africa to other jurisdictions. This shall be permitted only where one or more of the : (i) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the traveller (for example, to book travel or accommodation through a Vendor in a non-European country) or where the transfer is required or permitted by Applicable Privacy Laws.

13. **Return of data.** The Customer may in its absolute discretion by written notice require CT to return a complete copy of all the Customer's Personal Information to the Customer (or its nominee) by secure file transfer in such format as is reasonably notified by the Customer. The Customer shall be responsible for providing Data Subjects with any notice required under Applicable Privacy Laws in relation to such request.

14. **Data retention.** CT acknowledges that, as a general rule, Personal Information may not be kept indefinitely or longer than necessary for the intended Processing. The Customer Personal Information may only be retained for so long as is necessary to satisfy all applicable lawful bases for Processing set out in Section 11(1) POPIA, where applicable, and otherwise for such period as required by Applicable Privacy Laws, and always provided that CT shall ensure that such retained Personal Information is (i) kept confidential and protected against unauthorised access, disclosure or use and (ii) only Processed as necessary for the purpose specified in the Applicable Privacy Laws permitting its storage and other Processing and for no other purpose.

15. **Customer's right to audit.** CT shall keep or cause to be kept such information as is reasonably necessary to demonstrate compliance with its obligations under this Data Privacy Annexure and shall, upon reasonable notice during the term of the Agreement, make available to the Customer information necessary to demonstrate compliance with its obligations under this Data Privacy Annexure where such information is not subject to confidentiality restrictions owed to third parties. Without limiting the foregoing, CT shall make available to the Customer, on request: (i) a list of all Operators appointed by CT to Process the Customer's Personal Information; (ii) a copy of its most recent PCI DSS Attestation of Compliance, to the extent the Customer Personal Information includes any payment cardholder data; and (iii) a summary of the results of CT's latest internal data security audit for systems that are used to Process the Customer Personal Information. Any non-public documentation and information disclosed to the Customer in accordance with this paragraph shall be deemed proprietary and confidential information of CT. The Customer shall not disclose such documentation or information to any third party or use it for any purpose other than evaluating CT's compliance with this Data Privacy Annexure.

16. **Indemnity.** Each Party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including reasonable legal and professional costs and expenses) in connection with a regulatory or third party claim against the indemnified party arising out of or in connection with the breach of Applicable Privacy Laws by the indemnifying party, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it. The liability of the indemnifying party under this clause shall be subject to the limits set out in the Agreement.

17. **Survival**. The undertakings in this Data Privacy Annexure shall remain in force even after termination or expiration of the Agreement.

SCHEDULE TO THE DATA PRIVACY ANNEXURE: CT'S TECHNICAL AND ORGANISATIONAL MEASURES

1. **DATA SECURITY GOVERNANCE**

CT maintains internal organisational and governance procedures to appropriately manage information throughout its lifecycle. CT regularly tests, assesses and evaluates the effectiveness of its technical and organisational measures.

2. **PHYSICAL ACCESS CONTROL**

CT uses a variety of measures appropriate to the function of the location to prevent unauthorised access to the physical premises where Personal Information are Processed. Those measures include:

- Centralised key and code management, card-key procedures
- Batch card systems including appropriate logging and alerting mechanisms
- Surveillance systems including alarms and, as appropriate, CCTV monitoring
- Receptionists and visitor policies
- Locking of server racks and secured equipment rooms within data centres

3. **VIRTUAL ACCESS CONTROL**

CT implements appropriate measures to prevent its systems from being used by unauthorised persons. This is accomplished by:

- Individual, identifiable and role-based user account assignment, role-based and password protected access and authorisation procedures
- Centralised, standardised password management and password policies (minimum length/characters, change of passwords)
- User accounts are disabled after excessive failed log-on attempts
- Automatic log-off in case of inactivity
- Anti-virus management

4. **DATA ACCESS CONTROL**

Individuals that are granted use of CT's systems are only able to access the data that are required to be accessed by them within the scope of their responsibilities and to the extent covered by their respective access permission (authorisation) and such data cannot be read, copied, modified or removed without specific authorisation. This is accomplished by:

- Authentication at operating system level

- Separate authentication at application level
- Authentication against centrally managed authentication system
- Change control procedures that govern the handling of changes (application or OS) within the environment
- Remote access has appropriate authorisation and authentication
- Logging of system and network activities to produce an audit-trail in the event of system misuse
- Implementation of appropriate protection measures for stored data commensurate to risk, including encryption, pseudonymisation and password controls.

5. **DISCLOSURE CONTROL**

CT implements appropriate measures to prevent data from being read, copied, altered or deleted by unauthorised persons during electronic transmission and during the transport of data storage media. CT also implements appropriate measures to verify to which entities' data are transferred. This is accomplished by:

- Data transfer protocols including encryption for data carrier/media
- Profile set-up data transfer via secure file transfer methods
- Encrypted VPN
- No physical transfers of backup media

6. **DATA ENTRY CONTROL**

CT implements appropriate measures to monitor whether data have been entered, changed or removed (deleted), and by whom. This is accomplished by:

- Documentation of administration activities (user account setup, change management, access and authorisation procedures)
- Archiving of password-reset and access requests
- System log-files enabled by default
- Storage of audit logs for audit trail analysis

7. **INSTRUCTIONAL CONTROL**

CT implements appropriate measures to ensure that data may only be Processed in accordance with relevant instructions. Those measures include:

- Binding policies and procedures on CT employees
- Where Operators are engaged in the Processing of data, including appropriate contractual provisions to the agreements with Operators to maintain instructional control rights

8. **AVAILABILITY CONTROL**

CT maintains appropriate levels of redundancy and fault tolerance for accidental destruction or loss of data, including:

- Extensive and comprehensive backup and recovery management systems
- Documented disaster recovery and business continuity plans and systems
- Storage and archive policies
- Anti-virus, anti-spam and firewall systems and management including policies
- Data centres are appropriately equipped according to risk, including physically separated back up data centres, uninterruptible power supplies (including backup generators), fail redundant hardware and network systems and alarm and security systems (smoke, fire, water)
- Appropriate redundant technology on data storage systems
- All critical systems have backup and redundancy built into the environment.

9. **SEPARATION CONTROL**

CT implements appropriate measures to ensure that data that are intended for different purposes are Processed separately. This is accomplished by:

- Access request and authorisation processes provide logical data separation
- Separation of functions (production / testing)
- Segregation of duties and authorisations between users, administrators and system developer.