Schedule X
Data Privacy Addendum (Controller to Controller)

CORPORATE TRAVELLER™ Powered by melon

1. Definitions

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

1.1 **"Applicable Privacy Laws"** means all applicable data protection and privacy laws applicable to the Processing of Client Personal Data, including, when and where applicable, (a) the GDPR; (b) the UK Data Protection Act 2018; (c) the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC), (d) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426); (e) U.S. state and federal data protection laws, rules, or regulations including without limitation the California Consumer Protection Act of 2018 ("CCPA"); (f) the Personal Information Protection and Electronic Documents Act ("PIPEDA") and Canadian Anti-Spam Law ("CASL"), and (g) similar laws enacted anywhere in the world addressing the protection or the use, transmission, or other processing of Personal Data, 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 **"Client Personal Data"** means Personal Data provided to Corporate Travellers (CT) by Client, 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.

1.3 **"Controller"** means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

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

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

1.6 **"GDPR"** means the EU General Data Protection Regulation EU 2016/679, as implemented into national law and as amended, extended, re-enacted or applied by or under any other statute, law or enactment.

1.7 **"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.

1.8 **"Personal Data"** means any information relating to an identified or identifiable natural 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 information") may otherwise be defined in Applicable Privacy Laws).

1.9 **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data in CT's possession or control. Personal Data 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 Client Personal Data by unauthorised third parties; (ii) operational incidents which have an impact on the Processing of Client Personal Data; or (iii) any breach of this Data Privacy Addendum or Applicable Privacy Laws by CT, its employees or agents, to the extent that such breach affects the integrity and security of Client Personal Data or materially adversely impacts CT's obligations under this Data Privacy Addendum.

1.10 **"Processing"** means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by

automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, access, consultation, use, acquisition, transfer, hosting (via server, web, cloud, or otherwise), disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. 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.

1.11 **"Processor"** means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

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 Client's behalf to deliver travel related products and services to the Client.

In this Data Privacy Addendum, 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.

2. Parties as Controllers and compliance with Applicable Privacy Laws.

The parties acknowledge that, in order to provide the Services, CT must necessarily process Client Personal Data as a Controller. Each party shall act as a separate and independent Controller (and not as a joint Controller) in relation to all Client Personal Data 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 Client Personal Data and shall ensure that it has a lawful basis for all such Processing, where applicable. Where an affiliate of a party is a Controller or Processor of Client Personal Data under this Agreement, such party shall ensure that its affiliate complies with its obligations under the Applicable Privacy Laws and this Data Privacy Addendum as applicable.

Without limiting the foregoing, each party shall refrain from "selling" (as defined by the CCPA at Cal. Civ. Code § 1798.140(t), as it may be amended) or transferring Client Personal Data other than in compliance with the Applicable Privacy Laws.

3. Information provided to Data Subjects.

Prior to sharing any Client Personal Data with CT, Client shall provide all notifications required by Applicable Privacy Laws to the relevant Data Subject in each case with respect to the sharing of Client Personal Data with CT. Where CT collects Client Personal Data 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 Client Personal Data maintained by or for such party, and the parties will co-operate reasonably with each other in respect thereof.

6. Personal Data 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 Data Breach affecting Client Personal Data. In addition to complying with its notification requirements under Applicable Privacy Laws, CT shall promptly notify the Client of any technical, organisational or other incidents (including incidents at Processors) which have resulted in a Personal Data Breach in the sense of Art. 33 par. 1 GDPR affecting Client Personal Data. CT's notification of a Personal Data Breach to the Client must be comprehensive and include any information required under Art. 33 par. 3 GDPR and/or required by Applicable Privacy Laws, as and to the extent such information is available.

In the event of a Personal Data 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 Client Personal Data 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 Data 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 Data 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 Client Personal Data 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 Annexure to this Data Privacy Addendum. 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 Client Personal Data are properly qualified and trained and have committed themselves to keep Client Personal Data 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 Processors. If CT engages a third-party Processor to process Client Personal Data for the purpose of providing the Services, CT shall agree to written terms with the Processor that: (i) require the Processor only to process the Client Personal Data for the purpose of delivering the Services; (ii) require the Processor to implement appropriate technical and organisational security measures to protect the Client Personal Data against a Personal Data Breach; and (iii) otherwise comply with the requirements of Applicable Privacy Laws. CT shall remain responsible to the Client for any breach of this Data Privacy Addendum that is caused by an act, error or omission of the Processor.

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

12. Restricted transfers from the EEA or UK.

In order to enable the efficient and effective delivery of its Services, CT may from time to time transfer and Process Client Personal Data from the European Economic Area (and the United Kingdom) to other jurisdictions. This shall be permitted only where: (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 by applicable law; or (ii) CT has done all such acts and things as are necessary to ensure that any Client Personal Data transferred outside of the European Economic Area (and the United Kingdom) (whether to an CT Affiliate, a Processor, or otherwise) will remain adequately protected in accordance with the requirements of Applicable Privacy Laws. Client acknowledges that CT may ensure such adequate protection by executing the European Commission's Standard Contractual Clauses (or such other clauses as may be approved from time to time with regard to transfers of Personal Data out of the United Kingdom).

13. Return of data.

The Client may in its absolute discretion by written notice require CT to return a complete copy of all Client Personal Data to the Client (or its nominee) by secure file transfer in such format as is reasonably notified by the Client. The Client 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 Data may not be kept indefinitely or longer than necessary for the intended Processing. Client Personal Data may only be retained for so long as is necessary to satisfy all applicable lawful bases for Processing set out in Art.6 GDPR, where applicable, and otherwise for such period as required by Applicable Privacy Laws, and always provided that CT shall ensure that such retained Personal Data 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. Client'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 Addendum and shall, upon reasonable notice during the term of the Agreement, make available to the Client information necessary to demonstrate compliance with its obligations under this Data Privacy Addendum where such information is not subject to confidentiality restrictions owed to third parties. Without limiting the foregoing, CT shall make available to the Client, on request: (i) a list of all Processors appointed by CT to Process Client Personal Data; (ii) a copy of its most recent PCI DSS Attestation of Compliance, to the extent the Client Personal Data 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 Client Personal Data. Any non-public documentation and information disclosed to the Client in accordance with this paragraph shall be deemed proprietary and confidential information of CT. The Client 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 Addendum.

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 Addendum shall remain in force even after termination or expiration of the Agreement.

Annexure to Data Privacy Addendum: CT's Technical and Organisational Measures

Measures of pseudonymisation and encryption of personal data

- Encryption tools deployed in line with a central Encryption policy.
- Encryption tools leverage non-deprecated algorithms and approved products.
- Users educated on how to leverage encryption tools in line with an Encryption policy.
- Encryption of data in transit using TLS 1.2;
- Critical data at rest encrypted using AES 256;
- HR feed data is additionally encrypted using PGP during transmission and at rest on our SFTP server;
- Both disk level encryption and column level encryption employed;
- Third-Party Integration to Tokenization solution for some critical data;
- Cryptographic keys are protected against modification, loss and destruction through:
  - Centralised User Profiles for Authentication.
  - No Decryption or Re-Encryption in Case of Key Rotation or Expiration.
  - Maintain Comprehensive Logs and Audit Trails.
  - Common Encryption/Decryption Solution for the Entire Application.
  - Principle of Least Privilege.
  - Frequent Backups.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Confidentiality agreements within employee contracts as a requirement for employment;
- Maintenance of a complete ISMS of policies and procedures. These policies and procedures cover all aspects of confidentiality, integrity, and availability of data. Policies include (but are not limited to):
  - Access Control, Acceptable Use, Physical Security, Network Security, Encryption, Backup, Data Retention, Incident Management, Change Control, etc;
- Systems are backed up on, at minimum, a daily basis.
- Data files backed up on a separate system in case to protect data integrity and availability.
- All FCM technology is protected by commercial grade antivirus/antimalware software, with signatures updated daily.
- Disaster recovery plans in place, and tested, for key systems to enable recovery with business risk tolerances.
- 24x7x365 Monitoring of event data received from FCM staff workstations, servers, email and web logging sources.
- Vulnerability management plans are in place to ensure the timely detection and remediation of vulnerabilities within the FCM technology ecosystem.
- Firewall and IDS/IPS are implemented to detect and prevent any malicious activity at the network level.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Business continuity plan reviewed at least annually;
- Incident response plan reviewed at least annually;
- Data files and systems backed up on a separate system to protect data integrity. All FCM locations are protected by virus detection software;
- Disaster Recovery plan for systems with N+1 architecture where required to meet continuity requirements.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Internal and external audit program, audit reports and documentation.
- Testing of back up processes, disaster recovery, and business continuity procedures;
- Risk evaluation and system monitoring on a regular basis.

- Internal, external and application penetration testing conducted at least annually or after any significant change.
- Internal, external and application vulnerability scanning conducted at least monthly.
- Regular static code analysis performed on significant applications, all software engineers complete secure code training periodically.
- Private bug bounty program in place to continuously monitor external security posture of FCM.
- Continuous, proactive threat hunting across technology estate by expert threat hunters, informed by industry threats
- Security monitoring 24x7x365 conducted through SIEM solution, monitoring key servers, network infrastructure, workstation and user behaviour telemetry.

Measures for user identification and authorisation

- Access Control Policy that outlines the roles and responsibilities for both physical and logical access controls;
- User registration for starters and role changes, de-registration for leavers;
- Privileged access rights are restricted. Privileged access provided on an as-needed basis and must be approved by enterprise security before being created.
- Quarterly review of all privileged/superuser account access;
- Shared and generic accounts are against FCTG policy. Each individual is assigned a personal User ID to access authorised applications and system resources.
- Remote access to the corporate network requires MFA. MFA is also required to access the production environment and to perform administrative functions;
- Inactive sessions automatically close after 15 minutes;
- Access blocked after a set number of failed authentication access;
- Access granted based on a roles-based need-to-know basis in line with access policies;
- Differentiated access rights based on role (profiles, roles, transactions and objects);
- Monitoring and logging of accesses and role changes; entity and user behaviour analysis engine in place within SOC.
- Disciplinary action against employees who access personal data without authorisation;

Measures for the protection of data during transmission

- Customer HR feed data is encrypted using PGP during transmission and at rest on our SFTP server;
- Data is transferred using the following protocols: SFTP, HTTPS, or secure API over TLS 1.2 or higher;
- Intrusion detection and prevention systems in place. Active endpoint protection as well as anti-virus is in place across all endpoints and servers;
- Logging and 24x7x365 Monitoring controls for all critical infrastructure;
- All access for system components linked to a unique user in audit logs and that the actions are captured in logs.

Measures for the protection of data during storage

- Encryption standard requires the use of non-deprecated algorithms and approved products.
- Users educated on how to leverage encryption tools in line with Encryption standard.
- Critical data encrypted at rest using AES 256;
- Some critical data tokenized via Third-Party Tokenization service.
- Both disk level encryption and column level encryption employed;
- Cryptographic keys are protected against modification, loss and destruction through:
  - Centralised User Profiles for Authentication.
  - No Decryption or Re-Encryption in Case of Key Rotation or Expiration.
  - Maintain Comprehensive Logs and Audit Trails.

- Common Encryption/Decryption Solution for the Entire Application.
- Principle of Least Privilege.

- Frequent Backups.
- Access controls based on the principle of least privilege;
- Logical segmentation of customer personal data from data of other customers;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes;

Measures for ensuring physical security of locations at which personal data are processed

- Establishing access authorizations for employees and third parties with a need-to-know;
- Physical Security Policy to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities, including access to offices, rooms, and facilities. Our Physical Security Policy contains guidelines for working in secure areas, including technical closets and data centers. Areas holding critical or sensitive assets are designated as secure areas. Appropriate controls are in place, including (but not limited to): card swipe access, access logs, and supervision, when necessary.
- Our IT infrastructure is hosted by a large global hosting provider in geographically distributed facilities. Each facility is designed to run 24/7/365 and employs various measures to help protect operations from power failure, physical intrusion, natural disasters and network outages. These data centres comply with industry standards for physical security and availability.
- Security requirements with our subcontractors and sub suppliers, full acceptance of compliance with applicable legislative requirements around information protection, including physical security.

Measures for ensuring events logging

- Next generation SIEM with user and entity behaviour analysis,
- 24x7x365 Security operations centre monitoring log feeds, SIEM and broader monitoring health,
- Event logging sources compliant with PCI-DSS;
- End Point Detection and Response agents providing event telemetry from across technology estate,
- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;

Measures for ensuring system configuration, including default configuration

- Formal Change Control Policy to establish the rules for the creation, evaluation, implementation, and tracking of changes made to company Information Resources.
- Change control processes follow the Change Management document and apply to application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components.
- All changes are tested in a non-production environment before being implemented.
- Releases are managed through a Release to Production process to capture system configuration and support processes at time of release.
- All changes must be approved by the relevant and impacted stakeholders prior to deployment, therefore preventing impact on the availability of services provided to the Group;
- Baseline security configuration standards maintained and assets scanned to validate compliance,

Measures for internal IT and IT security governance and management

- Information security policies and procedures;
- Incident response plan;
- Regular internal and external audit;
- Review and supervision of information security program;
- Regular reporting of security risks, metrics and security strategy delivery to Board and Senior Management team,

Measures for certification/assurance of processes and products

- ISO27001 (UK operations)
- PCI DSS
- Cyber Essentials + (UK operations)

Measures for ensuring data minimisation

- Data Protection Impact Assessments undertaken
- Documentation regarding which data categories need to be processed;
- Ensure that the minimum amount of data is processed to fulfill the purpose of the processing;

Measures for ensuring data quality

- Personal data is kept accurate and up to date;
- Data is corrected upon request or where necessary;
- Subject Access Request process employed globally;
- Individuals provided access to their personal data to make changes/updates/corrections;

Measures for ensuring limited data retention

- Data retention schedule;
- Data retention policy;
- Personal data is deleted or irreversibly anonymized or otherwise deleted after expiration of the retention period;

Measures for ensuring accountability

- Internal policies and procedures;
- Privacy by design and by default;
- Records of data processing activities;
- Data Protection Impact Assessments, where required;
- Legitimate Interest Assessments, where required;
- Adequate agreements with third parties;
- Criteria for selecting the processors;
- Vendor onboarding process and questionnaire;
- Monitoring of contract performance;
- GDPR and InfoSec training program;

Measures for allowing data portability and ensuring erasure

- Personal data in made available upon request in an electronically portable format using industry standards;
- Secure disposal of information stored on magnetic and non-magnetic media that prevents potential recovery of the information;

Sensitive data

In addition to the measures above, the following measures are in place for transfers of sensitive data:

- Data use restricted solely for purposes of travel booking;
- Training of all staff in handling of sensitive personal data on employment and annually thereafter;
- Logging of data access;
- Access to staff limited by roles-based access.