Exhibit C

DATA PROCESSING ADDENDUM

1. INTRODUCTION

1.1 This Addendum sets out the additional terms, requirements, and conditions on which CSI (the **Vendor**) will process Four Seasons Personal Data when providing the Services under the Master Services Agreement entered into with any Property (collectively, the "Agreement" within this DPA).

1.2 In addition to terms defined within this Addendum and Schedules, the definitions and other provisions in Schedule 2 apply throughout. A reference to a Clause, Section, or Schedule is a reference to a Clause, Section, or Schedule of or to this Addendum, unless otherwise noted. The Schedules form part of this Addendum.

2. ROLES AND RESPONSIBILITIES

2.1 The Four Seasons management entity (**Property)** is responsible for determining the purposes and means by which Four Seasons Personal Data is processed at the property. Vendor acknowledges that it will process Four Seasons Personal Data solely on behalf of Property. For the avoidance of doubt, it is the parties' mutual understanding that: (a) Property is a controller of Four Seasons Personal Data; and (b) Vendor is a processor of the same.

2.2 Vendor acknowledges that the Customer (**Owner Entity)** has entered into this Addendum for the benefit of Property. The rights granted to Property under this Addendum shall be directly enforceable by Owner Entity on behalf of Property. Without limiting the foregoing, a person who is not a party to this Addendum may not otherwise enforce any of its terms unless expressly stated in this Addendum or the Agreement. If and to the extent Owner Entity is not able to recover a loss incurred by Property under this Addendum on the basis a claim to recover that loss is not, by operation of law or decision of a court, deemed to be enforceable by Owner Entity itself, then Property shall be entitled to enforce this Addendum against Vendor in its own right, subject always to the provisions of this Addendum and the Agreement.

2.3 Vendor and Property shall comply with their respective obligations under Data Protection Laws in relation to the processing of Four Seasons Personal Data under, or in connection with the performance of, this Addendum and related Agreement. Nothing in this Addendum shall relieve either Vendor or Property of its own responsibilities and liabilities under Data Protection Laws.

3. VENDOR USE OF FOUR SEASONS PERSONAL DATA

3.1 *Compliance with instructions*. Vendor shall:

(a) only process Four Seasons Personal Data in accordance with the Agreement and any written instructions provided by Property from time to time; not collect, process, retain, use or disclose Four Seasons Personal Data for any commercial purpose other than as set forth in and pursuant to the Agreement;

(b) not sell, disclose, release, transfer, make available or otherwise communicate any Four Seasons Personal Data to any third party without the prior written consent of Property, except where specifically permitted under Section 7 or where required by applicable law

(in such cases, Vendor shall comply with its obligations under Clauses 6.3 and 6.4). To obtain such consent, Vendor shall send an email to corporate.it.security@fourseasons.com; and

(d) promptly notify Property if it is unable to follow Property's instructions, or if, in Vendor's opinion it would be unable to process Four Seasons Personal Data without breaching Data Protection Laws.

3.2 *Sub-processor instructions*. Subject to Section 7, Property authorizes Vendor to instruct sub-processors to process Four Seasons Personal Data for the purpose of exercising Vendor's rights and performing its obligations under this Addendum and the Agreement.

3.3 *Purpose limitation, accuracy, and duration of processing*. Vendor shall process Four Seasons Personal Data in accordance with, and only for the purposes specified in, Schedule 1. Vendor further agrees that processing shall only take place for the duration specified in Schedule 1. Vendor shall inform Property if it becomes aware that any Four Seasons Personal Data is inaccurate or has become outdated. Such notice shall be sent to privacy.officer@fourseasons.com.

4. SECURITY OF PROCESSING

4.1 *Maintain appropriate technical and organizational security*. Vendor shall, considering the state of the art and the nature, scope, context, and purpose of processing, as well as the potential risk to the rights and freedoms of natural persons due to the processing, implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk with respect to Four Seasons Personal Data and other Confidential Information. Such assessment shall account for the risk of unauthorized or unlawful processing of, as well as the accidental or unlawful loss, alteration, unauthorized disclosure, or destruction of, Four Seasons Personal Data and other Confidential Information.

4.2 *Sensitive data*. If Vendor's processing involves Four Seasons Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (**Sensitive Data**), Vendor shall apply any additional safeguards included in the Security Measures (Schedule 3) for Sensitive Data.

4.3 *Adherence to Security Measures*. Without limiting Clauses 4.1 or 4.2, Vendor shall always implement at least the measures set out in the Security Measures (Schedule 3).

4.4 *Vendor Personal Data Breach response*. Upon becoming aware of an actual or suspected Personal Data Breach, the Vendor shall take reasonable steps to investigate, and mitigate the effects of, the Personal Data Breach. Vendor shall notify Property of the incident pursuant to Clause 4.5. Property shall have sole control over the content, timing, and method of distribution of any notice sent to any data subject(s), supervisory authority(ies), and/or regulator(s) (collectively, **Notice Recipients**). Except as required by applicable law or regulation, Vendor may not send notifications to any Notice Recipients without Property's express written approval. At Property's request, Vendor shall notify data subject(s) on behalf of Property and Vendor shall function as the primary contact point for inquiries and complaints related to the Personal Data Breach.

4.5 *Notification of Personal Data Breach to Property*. Vendor shall notify Property without undue delay, and in any event within 48 hours, after becoming aware of or having reasonable suspicion

of an actual or suspected Personal Data Breach involving Four Seasons Personal Data. Vendor shall first attempt to notify Property by calling Four Seasons' incident response hotline at +1 613 416 8000. If Vendor cannot reach Property over the phone, the initial notice must be sent via email to corporate.it.security@fourseasons.com and privacy.officer@fourseasons.com. That initial notice sent via e-mail should only inform Property of the potential Personal Data Breach and include contact information for an individual from whom Property can obtain additional details of the incident. Vendor shall be prepared to provide the following information regarding the Personal Data Breach, including, if available, details of: (a) how the incident occurred and the facts surrounding it; (b) the categories of Four Seasons Personal Data and number of data records affected, (c) details of individuals and the approximate number of individuals and records affected including, where possible, the country of residency of the affected data subjects; (d) the likely consequences of the incident, if known; and (e) the measures taken or proposed to be taken to address the incident, prevent future occurrence and to mitigate its possible adverse effects. Where it is not possible to provide all information at the same time, further information shall be provided subsequently as it becomes available. Property shall be entitled at any time, but only on request, to require the Vendor to provide the foregoing details in a written report.

4.6 *Cooperation with Property's review*. Upon Property's written request, Vendor shall provide Property with co-operation and assistance (including access to appropriate facilities, employees, records, information, and systems) reasonably requested by Property related to a Personal Data Breach to enable Property to (a) take appropriate remedial measures Property deems prudent; (b) send notices to Notice Recipients; and (c) respond to any subsequent review by or inquiries from any relevant Data Protection Authority, any other public authority, or any other third party concerned, regardless of whether such responses are required by applicable law.

4.7 *Costs associated with Personal Data Breach*. Vendor agrees to reimburse Property for costs necessarily incurred with Property's response to a Personal Data Breach impacting Four Seasons Personal Data when such breach relates to the Vendor's, or Vendor's sub-processors, processing of Four Seasons Personal Data (**Data Breach Costs**). For the avoidance of doubt, such Personal Data Breach includes the unauthorized acquisition of or access to Four Seasons Personal Data processed on Vendor's or Vendor's sub-processor's systems. Vendor agrees to reimburse Data Breach Costs related to Property's review and remediation of the incident, notification to Notice Recipients, provision of identity protection or fraud protection services to impacted data subjects (at Property's discretion), fines imposed by Data Protection Authorities related to the Personal Data Breach, and professional fees incurred related to the breach, including reasonable attorney's fees and fees from public relations vendors, customer notification service providers, and forensic investigators. Vendor will not be obligated to reimburse Property for costs identified in this Clause 4.7 if the Personal Data Breach is caused by Property's negligence or misconduct. The maximum amount of Data Breach Costs that Vendor will be liable to reimburse Property for hereunder will be limited to $1 million U.S. dollars, provided that Vendor's aggregate liability to all Properties managed by Four Seasons (including the Property) shall not exceed $2 million US dollars (**Data Breach Costs Cap**).

4.8 *Non-Exclusive Remedies for Breach*. Vendor's failure to meet the requirements in this Addendum with respect to the security of Four Seasons Personal Data or other Confidential Information, including the requirements outlined in the Security Measures (Schedule 3) is a material breach of the Agreement for which Owner Entity, at its option, may terminate the Agreement on written notice to Vendor in accordance with the Agreement.

5. COMPLIANCE DOCUMENTATION, ASSISTANCE, AND AUDIT

5.1 *Assistance with Property's privacy assessments*. Upon Property's written request, Vendor shall provide reasonable assistance to Property regarding the assessment of the privacy impact related to Vendor's processing of Four Seasons Personal Data when such assessment is either: (a) required or prudent under Data Protection Laws; or (b) conducted by Property to comply with its internal processes and procedures. Such assistance may include providing information to Data Protection Authorities upon Property's request.

5.2 *Demonstrate compliance with this Addendum*. Subject to compliance with applicable laws, Vendor shall, upon Property's written request, provide all information necessary to demonstrate compliance with this Addendum, including information provided by sub-processors. Property may request to receive information verbally, or in writing; such information includes, but is not limited to, details regarding the technical and organizational measures employed by Vendor and/or a sub-processor related to the processing of Four Seasons Personal Data. Such information regarding technical and organizational measures includes, without limitation, a summary of a routine assessment conducted by the Vendor to determine if its information security program complies with the SSAE 18 standard, ISO/IEC 27001, or other alternative standards that are substantially equivalent to those standards. Property shall maintain all information related to such assessments, including any written summaries, as Vendor's Confidential Information and will not distribute or allow any third party (other than Property's independent auditors) to use any such information without the prior written consent of Vendor, unless required by applicable law.

6. INDIVIDUAL RIGHTS, DATA PROTECTION AND PUBLIC AUTHORITY INQUIRIES

6.1 *Notice of individual rights request*. If an individual makes a written, electronic, or verbal request to Vendor to exercise any of their rights under Data Protection Laws in relation to Four Seasons Personal Data, Vendor shall forward the request to Property promptly and in each case within three days from the date on which Vendor received the request. Notification must be sent to privacy.officer@fourseasons.com. Vendor shall not respond to such requests itself unless it has been authorized to do so by Property in writing or is otherwise required by applicable law or regulation.

6.2 *Assistance related to rights requests*. Upon Property's reasonable written request, Vendor shall provide Property with all co-operation and assistance requested by Property in relation to any individual request to exercise their rights under Data Protection Laws. This includes, but is not limited to, implementing appropriate technical and organizational measures to fulfil and respond to such requests.

6.3 *Notification of and assistance with Data Protection Authority inquiry*. Vendor shall immediately notify Property if it is subject to any inspection or investigation conducted by any Data Protection Authority regarding the processing of Four Seasons Personal Data. Notification must be sent to privacy.officer@fourseasons.com. Vendor shall assist Property in responding to any investigation, inspection, notice, or communication from any Data Protection Authority or other authority in relation to the processing of Four Seasons Personal Data.

6.4 *Notice of request from other public authority.* Vendor shall keep Four Seasons Personal Data confidential in accordance with the terms of this Addendum except where disclosure is required by applicable law, in which case the Vendor shall, where not prohibited by applicable law, immediately notify Property of any such requirement (and in any event before such disclosure).

7. SUB-PROCESSORS

7.1 *General written authorization*. Notwithstanding any provisions governing the appointment of sub-contractors in the Agreement, Property provides general authorization for Vendor to engage other processors (each a **sub-processor**) to process Four Seasons Personal Data. Vendor shall:

(a) before disclosing Four Seasons Personal Data to any sub-processor, enter into a contract with that sub-processor containing terms equivalent to those in this Addendum;

(b) be responsible for all acts and omissions of any sub-processor as fully as if they were the acts and omissions of Vendor or its employees or agents; and

(d) except where expressly provided otherwise, be Property's sole point of contact for the performance of Vendor and Vendor's sub-processor's obligations under this Addendum.

An agreed list of sub-processors can be found in Schedule 1. Vendor shall inform Property no less than 60 days in advance of any intended changes concerning the addition or replacement of sub-processors to those already approved, so giving Property the opportunity to object. Such notifications must be sent to corporate.it.security@fourseasons.com. If Property notifies Vendor in writing that it objects to Vendor's proposed appointment of an additional or alternative sub-processor, Property may terminate the Agreement.

7.2 *Confidentiality obligation*. Before disclosing Four Seasons Personal Data to any of its agents or sub-processors, Vendor shall ensure that those persons:

(a) have taken appropriate training in data protection; and

(b) are bound to hold the Four Seasons Personal Data in confidence, to at least the same standard as required under this Addendum.

8. Intentionally deleted

9. CONSEQUENCES OF TERMINATION AND EXPIRY

9.1 Unless expressly stated otherwise in this Addendum or the Agreement, upon termination or expiry of the Agreement, Vendor shall, and shall procure that each sub-processor shall immediately cease to use Four Seasons Personal Data; and

(a) at Property's option and in accordance with Property's instructions:

(i) return Four Seasons Personal Data to Property; and/or

(ii) delete the Four Seasons Personal Data and other Confidential Information, as well as all copies and extracts of Four Seasons Personal Data and other Confidential Information unless required to retain a copy in accordance with applicable laws or any written data retention policy, but only for as long as is set forth in such policy. Vendor shall destroy all data in a fashion that renders it unrecoverable, and which adheres to NIST SP 800 88 Rev 1 (or a successor standard) or equivalent data destruction standard. Data destruction shall be completed on all forms of data and in all locations excluding system backups. A confirmation of data destruction will be provided to Property upon written request;

(b) if Four Seasons Personal Data is contained in an electronic file created pursuant to any routine backup or archiving procedure which renders it inaccessible or incapable of

deletion, anonymize such file wherever possible; if anonymization is not possible, the data may be retained in line with Vendor's retention periods so long as it is not generally accessible beyond the need for disaster recovery or similar operations or to comply with applicable law; and

(c) to the extent that any Four Seasons Personal Data or other Confidential Information remains in the possession of Vendor following a request for return or destruction of same from Property, Vendor shall continue to process that Property data in accordance with applicable law and this Addendum.

9.2 *Survival.* On expiry or termination of this Addendum, this Section 9 shall survive and continue in full force and effect. Vendor shall continue to ensure compliance with this Addendum until the Four Seasons Personal Data and Confidential Information is deleted or returned in accordance with this Section 9.

10. GOVERNING LAW AND JURISDICTION

10.1 *Governing law*. Subject to the UK SCCs, or EU SCCs (if applicable), this Addendum and any non-contractual obligations arising out of or in connection with it or its subject matter or formation shall be governed by, and construed in accordance with, the law specified in the Agreement.

11. MISCELLANEOUS

11.1 *No transfer of rights*. The parties to the Agreement acknowledge that nothing in this Addendum constitutes a transfer or assignment of any rights in Four Seasons Personal Data (including any intellectual property rights) unless otherwise expressly set out in the Agreement.

11.2 *Hierarchy*. If there is any conflict or inconsistency between a term in the body of this Addendum and a term in the Agreement, or in any of the Schedules or other documents referred to or otherwise incorporated into this Addendum, the term in the body of this Addendum shall take precedence.

11.3 *Variability*. Subject to any change control procedure contained in the Agreement, any variation of this Addendum shall not be binding on the parties to the Agreement unless set out in writing, expressed to vary this Addendum, and signed by authorized representatives of Vendor and Owner Entity.

11.4 *Severability*. The provisions contained in each Section and Clause of this Addendum shall be enforceable independently of each of the others and their validity shall not be affected if any of the others are invalid. If any of those provisions is void but would be valid if some part(s) of the provision were deleted, the provision in question shall apply with such modification as may be necessary to make it valid.

SCHEDULE 1

DESCRIPTION OF PROCESSING AND TRANSFERS

ONCE IN TIME APPLICATION SUBMISSIONS:

Duration of processing	Unless stated otherwise in this Addendum, or agreed in writing between the parties, Four Seasons Personal Data will be processed for the duration stated in the Agreement.
Nature and purpose of processing	For the purpose of the provision of Services by Vendor under the Agreement.
Frequency of transfer	One-off transfer at time of application, upon customer requested changes or upon request by CSI for KYC purposes
Maximum retention period	Four Seasons Personal Data shall be retained in accordance with the Data Recipient's data retention standards.
Individuals/data subjects:	*Mark all that apply.* ☒ Four Seasons employees ☐ Four Seasons contractors ☐ Four Seasons guests ☐ Members of the public ☒ Other – please specify: Hotel Owners and Property control persons
Categories of Four Seasons Personal Data:	*Mark all that apply:* ☒ Title or gender ☒ Name ☒ Email address ☒ Mailing address ☒ Telephone or mobile number ☐ Citizenship or nationality or place of birth (provide details below) ☒ Date of birth or age ☐ Marital status ☐ Number of children ☐ Stay/purchase history ☐ Payment card details ☐ Credit status or rating ☒ Digitised electronic signature ☐ Vehicle licence plate number ☐ Photograph of an individual

	☐ Geo-location data ☐ IP address ☐ Other online identifier (e.g., cookie data) ☐ Employee ID ☒ National Insurance, Social Security, or similar number ☒ Government issued ID numbers (passport, driving licence, etc.) ☐ Video streams or recordings (e.g., CCTV) ☐ Audio streams or recordings (e.g., CCTV) ☐ Recruitment details (e.g., curriculum vitae or similar career history, interview records, employment contracts, etc. (exc. background checks (to be covered below))) ☐ Employment details (e.g., performance reviews, grievance information, employment contracts, etc. (exc. payroll information and health data (to be covered below))) ☐ Payroll information (e.g., salary and benefits, tax codes, bank account details, expense records) ☒ Other – please specify: Ownership %
Sensitive Data:	*Mark all that apply:* ☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs, or trade union membership ☐ Genetic data ☐ Biometric data for the purpose of uniquely identifying a natural person ☐ Data concerning health (e.g., smoking preference, medical symptoms (such as anxiety, high blood pressure, dizziness, nausea, or morning sickness), medical conditions or past surgeries collected prior to spa treatments, results of examinations and medical treatments, vaccine status, Body Mass Index, etc.) ☐ Data concerning a person's sex life or sexual orientation ☐ Disciplinary information ☐ Criminal record ☒ None - the personal data being processed does not include any of the above Sensitive Data.

VENDOR PAYMENT DETAILS:

Duration of processing	Unless stated otherwise in this Addendum, or agreed in writing between the parties, Four Seasons Personal Data will be processed for the duration stated in the Agreement.
Nature and purpose of processing	For the purpose of the provision of Services by Vendor under the Agreement.
Frequency of transfer	Continuous
Maximum retention period	Four Seasons Personal Data shall be retained in accordance with the Data Recipient's data retention standards.
Individuals/data subjects:	*Mark all that apply.* ☐ Four Seasons employees ☐ Four Seasons contractors ☐ Four Seasons guests ☐ Members of the public ☒ Other – please specify: Hotel Owners/Property/vendors
Categories of Four Seasons Personal Data:	*Mark all that apply:* ☒ Title or gender ☒ Name ☒ Email address ☒ Mailing address ☒ Telephone or mobile number ☐ Citizenship or nationality or place of birth (provide details below) ☐ Date of birth or age ☐ Marital status ☐ Number of children ☐ Stay/purchase history ☒ Payment card details ☐ Credit status or rating ☒ Digitised electronic signature ☐ Vehicle licence plate number ☐ Photograph of an individual ☐ Geo-location data ☐ IP address ☐ Other online identifier (e.g., cookie data) ☐ Employee ID ☐ National Insurance, Social Security, or similar number ☐ Government issued ID numbers (passport, driving licence, etc.)

	☐ Video streams or recordings (e.g., CCTV) ☐ Audio streams or recordings (e.g., CCTV) ☐ Recruitment details (e.g., curriculum vitae or similar career history, interview records, employment contracts, etc. (exc. background checks (to be covered below))) ☐ Employment details (e.g., performance reviews, grievance information, employment contracts, etc. (exc. payroll information and health data (to be covered below))) ☐ Payroll information (e.g., salary and benefits, tax codes, bank account details, expense records) ☒ Other – please specify: Invoice and remittance details
Sensitive Data:	*Mark all that apply:* ☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs, or trade union membership ☐ Genetic data ☐ Biometric data for the purpose of uniquely identifying a natural person ☐ Data concerning health (e.g., smoking preference, medical symptoms (such as anxiety, high blood pressure, dizziness, nausea, or morning sickness), medical conditions or past surgeries collected prior to spa treatments, results of examinations and medical treatments, vaccine status, Body Mass Index, etc.) ☐ Data concerning a person's sex life or sexual orientation ☐ Disciplinary information ☐ Criminal record ☒ None - the personal data being processed does not include any of the above Sensitive Data.

Permitted sub-processors

Permitted Sub-processors	**Nature and duration of processing**	**Address**	**Contact person (name, position, contact details)**
AWS	Hosts Paysystems and		N/A
Sendgrid/RackSpace	Data storage		N/A

SCHEDULE 2: DEFINITIONS

In this Addendum, the terms **controller**, **personal data**, **processing**, and **processor** shall have the meaning given to them in Data Protection Laws. Other defined terms are as follows:

Confidential Information is defined pursuant to the Agreement;

Data Protection Authority means the relevant competent authority responsible for data privacy and protection, which may or may not be where Property or Vendor is established;

Data Protection Laws means any law, enactment, regulation, or order concerning the processing of data relating to living persons including each to the extent applicable to the activities or obligations of Property, Owner Entity, and Vendor under or pursuant to this Addendum;

Data Recipient means the Vendor or a third party who receives Four Seasons Personal Data from, or is given access to Four Seasons Personal Data by, the Data Sender under, or in connection with, the terms of this Addendum;

Data Sender means Property, or Vendor, in cases where the entity transfers (via international transfer or otherwise) Four Seasons Personal Data to a Data Recipient or provides access to Four Seasons Personal Data to a Data Recipient under or in connection with this Addendum;

Four Seasons Personal Data means any personal information or personal data (each as defined in applicable Data Protection Laws) which is: (i) supplied by or on behalf of Property to Vendor (including where Vendor has access to personal data held by Property or a processor on its behalf), (ii) which Vendor collects, generates, or otherwise processes on behalf of Property; or (iii) which Vendor otherwise processes under or in connection with providing the Services or performing an obligation under the Agreement, as further described in Schedule 1;

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Four Seasons Personal Data transmitted, stored, or otherwise processed by the Vendor or Vendor's sub-processors;

;

Security Measures means the security measures outlined in Schedule 3; and

Services mean the services provided under the Agreement.

SCHEDULE 3

SECURITY MEASURES

Throughout the term of the Agreement, and at all times in connection with its actual or required performance of the Services thereunder and in compliance with all applicable laws, Vendor shall maintain and enforce an information security program, including incident response, escalation, and physical, technical, organizational, and contractual security policies and procedures with respect to its processing of Property's Confidential Information (including Four Seasons Personal Data) that meet or exceed Property's data security requirements set forth in this Schedule, the Addendum, and the Agreement. Any such practices and standards must be at least as protective as industry standards in all jurisdictions where Property and Vendor carry on activities under the Agreement. Without limiting the foregoing, Vendor agrees that it has in place, and will have in place during the term of the Agreement, the following security measures:

1) *Security monitoring and governance*. Vendor shall maintain measures to effectively monitor, detect and mitigate attacks, break-ins, potential threats, and other malicious activities launched against any electronic systems, including without limitation, its network, its operating system, all databases, and any and all applications and underlying technologies (collectively, the **Systems**), associated with providing the Services. These measures include, without limitation, collecting, managing, and protecting audit logs (**Audit Logs**) and following up on all anomalies detected. Vendor represents and warrants that its Audit Logs: (a) track all actions taken in connection with the Systems, including without limitation, all changes to configuration of servers, networks, databases, and/or business applications containing Four Seasons Personal Data, including changes to the Four Seasons Personal Data itself (each an **Action**); (b) with respect to each Action, track, at a minimum, the time, date, and type of Action taken; (c) are configured such that all Actions can be traced to an individual; and (d) are kept for at least one (1) year and protected on separate, dedicated storage devices.

2) *Logical access controls*. Vendor shall control access to its Systems through at least the following means: (a) adhering to policies and procedures that comply with PCI-DSS Requirement 8 (available at www.pcisecuritystandards.org); (b) restricting access to all Systems, granting access only to those users that have a need for such access in order to perform their roles; (c) having a process for on-boarding and off-boarding staff to appropriately control and restrict access to all Systems; (d) with respect to employees, contractors, agents, or other representatives (**Personnel**) who have a material role in processing Four Seasons Personal Data, submitting such Personnel to background verification (as permitted by local laws, regulations, ethics, and contractual constraints); (e) creating all accounts using the "least privilege" principle, and granting all users only the necessary privilege required for their role; and (f) using Multi-Factor Authentication to protect all accounts that have administrative privilege to access the Systems used to provide the Services.

3) *Physical access controls.* Vendor shall have in place, and will have in place during the length of the Agreement, measures to ensure physical security controls are in place for all data centres, hosting providers, corporate offices or any location where Four Seasons Personal Data may reside, and will ensure that physical access to such non-public locations is restricted and closely monitored, including without limitation that Vendor (i) has, and will follow, policies and procedures that address the purpose, scope, roles, responsibilities and compliance measures required for physical and environmental security of its Systems, including without limitation that such policies and procedures address security perimeter and entry controls, working in secure areas, equipment security, cabling security, fire detection and suppression, and room temperature; and (ii) controls physical access to such facilities containing information systems, maintains records of access by approved personnel, requires sign-in sheets for all

visitors, periodically reviews such logs, investigates all violations or suspicious activities, and takes action to address issues or concerns identified.

4) *Information security awareness*. Vendor shall have in place an information security awareness program for all of its Personnel to protect its Systems and to ensure the confidentiality, integrity, and availability of data. Such program provides Personnel with training, reference materials, support, and reminders that enable them to appropriately protect data assets and obligates Personnel to understand and agree to abide by the policies that affect their areas of activity.

5) *Annual incident response testing*. Vendor shall facilitate an annual incident response test and modify its related plans and/or policies in connection with the lessons learned from such tests, including that evidence of such testing and the modified plans and/or policies in consequence of such tests will be provided to Property upon request.

6) *Cryptographic standards and key management*. Vendor shall utilize cryptographic standards mandating authorized algorithms, key length requirements, and key management processes that are consistent with or exceed then-current industry standards, including NIST recommendations, and utilize hardening and configuration requirements consistent in approach with then-current industry standards, which at a minimum shall be Center for Internet Security (**CIS**) recommendations. Vendor shall provide security key management and other facilities to ensure that encrypted data is not lost or irretrievable should the encryption keys become unavailable.

7) *Encryption in transit and at rest*. Vendor shall ensure that Four Seasons Personal Data, whether in transit or at rest, including storage within databases, is protected at all times by using end to end cryptographic protocols, including without limitation that Vendor shall implement encryption in transit that supports the latest Transport Layer Security (**TLS**) protocol, and has the ability to block TLS protocols older than the current version minus 1 (e.g., if TLS 1.3 is the current version, TLS 1.1 can be blocked). For the avoidance of doubt, the in-transit encryption protocol requirements apply to all communication that transmits Four Seasons Personal Data and/or Confidential Information. Vendor shall, without limitation, encrypt data at rest using AES-256 encryption or the most recent industry standard level of encryption. Vendor shall never decrypt Four Seasons Personal Data in non-production systems and/or test environments.

8) *Vulnerability management program*. Vendor shall execute (a) third-party penetration tests by an accredited vendor on an annual basis with all critical vulnerabilities patched within fifteen (15) days and high vulnerabilities patched no later than thirty (30) days after being identified by such tests; and (b) vulnerability assessments on an, at least, semi-annual basis with all critical and high vulnerabilities patched no later than thirty (30) days after being identified by Vendor. Upon request by Property, Vendor shall provide Property with evidence that an external network and applicable penetration tests have been completed and shall provide Property with an executive summary which includes the scope of the assessment, major findings, and remediation status. Such reports shall be considered Vendor's Confidential Information.

9) *Change management*. Vendor maintains a change management process to control any changes made to its products, services, and Systems, and to keep its Systems up-to-date with the latest upgrades, bug fixes, new versions, and other modifications in line with industry best practices. Vendor represents and warrants to Property that all changes (a) are documented, reviewed, tested, and approved in accordance with Vendor's written policies; and (b) will be implemented in a seamless manner to avoid or minimize service degradation to Property.

10) *Routine maintenance*. Vendor shall provide routine maintenance to its systems, including tasks necessary to correct ordinary defects in the systems, tasks necessary to ensure continued day-to-day operation of the systems, and tasks necessary to affect other minor modifications and improvements to the system.

11) *IT Service Continuity*. Vendor shall have in place a defined and agreed recovery point objective (**RPO**) and recovery time objective (**RTO**) for their Services, and based on the RPO and RTO, shall maintain and will follow an at least industry standard disaster recovery and business continuity plan for the restoration of critical processes and operation of the Services (the **BCP**), which contemplates, without limitation, the provision and maintenance of necessary controls such as backup power to facilitate an orderly shutdown process, fire detection and suppression, temperature and humidity controls, water damage detection and mitigation, network availability, and infrastructure health controls. Any Force Majeure provisions of the Agreement shall not limit Vendor's obligations in this Clause.

12) *Single Sign-On Support (if applicable to Vendor)*. In cases where Vendor will provide access to a platform wherein Property's employees, contractors, or other individuals will access the platform via log-in credentials, Vendor will provide Property with federated single sign on capabilities (**FSSO**) that will allow Property to internally control the authentication process to the Vendor platform. Vendor shall accept the credentials (as more fully described below, the **Identifying Credentials**) of each participant as accurately identifying the participant and then provide the latter with access to the platform in accordance with the following: (a) Property shall be responsible for the establishment, implementation and oversight of the rules, requirements and procedures relating to the provisioning, de-provisioning, distribution, selection, use and safeguarding of the Identifying Credentials (such as the user ID and passwords) and for the verification of the identity of each participant and its respective level of access authorization for the platform and Property agrees that it shall utilize at least "standard industry practices" in regard to password policies, user provisioning and de-provisioning, and the creation of persistent, unique and static user ID's, and therefore Vendor shall not have any responsibility to authenticate participants or otherwise verify their identity or authorized access levels; and (b) the FSSO shall utilize either the "Security Assertion Mark-up Language 2.0" (**SAML**), or another SSO methodology deemed acceptable by Property as evidenced by Property in writing (Vendor agrees to contact corporate.it.security@fourseasons.com to identify other acceptable SSO configurations and obtain such written approval). Property acknowledges it is responsible for procuring, at its expense, all hardware and software necessary to utilize the FSSO.

13) *Remote access (if applicable to Vendor)*. In cases where Vendor will access Property's computer systems remotely, it will do so only using the remote access technology currently approved for use by Property. Contact corporate.it.security@fourseasons.com for more information.

14) *Administration of Property's Systems (if applicable to Vendor*). In cases where Vendor will administer Property's computer systems, Vendor shall ensure that any accounts used to administer Property's computer systems are unique to Property and are not shared across multiple clients.

15) *Provisions for Cardholder Data*. Vendor shall adhere to the following requirements with respect to its' storage, processing, handling or transmission of cardholder data in any manner, whether by Vendor itself, or through a sub-processor or other agent of Vendor. The term **Cardholder Data** refers to the number assigned by the card issuer that identifies the cardholder's account, as well as all other data related to the payment card, including, but not limited to, expiration date and CVV code. Cardholder Data shall also include all of the cardholder's Four Seasons Personal Data. Vendor: (a) shall at all times while accessing or holding Cardholder Data, comply with the current version of Payment Card Industry (**PCI**) requirements for Cardholder Data that are prescribed in the PCI Data Security Standard (**PCI-**

DSS) - copies of the current PCI-DSS requirements documentation are available on the www.pcisecuritystandards.org website; (b) hereby represents and warrants that it has received certification and is and shall be and remain certified PCI compliant at all times throughout the Term of this Agreement; (c) acknowledges and agrees that it will have access to Cardholder Data and that such Cardholder Data may only be used for the purposes set out in this Agreement and Vendor will not copy, use, alter or delete Cardholder Data for any purpose except as herein required or as required by applicable law, and in such case, only after sending notice to Property at corporate.it.security@fourseasons.com; (d) will not transfer Cardholder Data outside the Property environment for any purpose; (e) shall, in the event of an attempt at access, a breach or intrusion of, or otherwise unauthorized access to, Cardholder Data, immediately notify Property pursuant to the terms in the Addendum; (f) shall maintain appropriate business continuity procedures and systems to ensure security and integrity of Cardholder Data in the event of a disruption, disaster or failure of Vendor's primary data systems; (g) shall provide an Attestation of Compliance from an arm's length third party approved by Property (**Attestation**) in the current form set by PCI-DSS within 30 days of execution of this Agreement and annually thereafter during the Term of this Agreement, upon written request; failure to provide any such Attestation is a material breach of the Agreement entitling Property to immediately terminate the Agreement without penalty or liability of any kind, and in such circumstances Property shall have no further obligations to Vendor; (h) agrees to manage and be fully responsible for the high level PCI requirements and the requirements as outlined in the chart at Annex 1 attached hereto and Vendor agrees that its Attestation shall include an audit of the obligations of Vendor set out in such chart; and (i) its successors and assigns shall comply with the PCI-DSS Requirements including after termination of this Agreement for as long as Cardholder Data is in the possession of Vendor, its successors or assigns.

16) *Multi-Factor Authentication (**MFA**) standards*. Vendor will support the following requirements for MFA, provided that Vendor acknowledges that the MFA standards are subject to change on written notice from Property, in Property's discretion: (a) Vendor will use the following authentication methods: offline time-based verification codes (TOTP); Hardware tokens, such as Yubico YubiKey; X.509–based certificates; Legacy authentication methods, such as SMS, security questions, or email; Open Standards Support; SAML; OpenID Connect; and OAuth2; and (b) Vendor will ensure it is capable of sending system logs for monitoring, including without limitation that it will: have the ability to send authorization events to a third-party SIEM solution, include out-of-the-box reports and audit trails, support effecting authorization system change based on authorization events, and provide real-time information about access attempts.

17) *Firewall/Perimeter defense requirements*. Vendor represents, warrants and covenants, that throughout the Term, it will take the following measures to protect the Services (whether they are offered natively on a cloud platform or acquired through other means) from unauthorized use and/or access, distributed denial of service (**DDoS**) attacks, malicious actors, malware, and access through utilization of Cloud Security Services, including, without limitation by: (a) maintaining a firewall at all logical demilitarized zones (**DMZ**) and Internet connection points, with access control restricted to that required for authorized use of Vendor's Systems; (b) implementing web application firewalls for all web applications to filter, monitor, and block HTTP traffic to and from all web applications; (c) using threat protection devices and analytic services, such as, Intrusion Detection Systems (**IDS**), Intrusion Prevention Devices (**IPD**) and Threat Analytics Platforms (**TAP**), as part of its network security strategy, in addition to the firewalls; (d) monitoring all threat detection logs on a regular basis to detect likely and/or actual unauthorized access attempts to Four Seasons Personal Data; (e) restricting and controlling wireless network access using industry standard wireless security protocols; (f) restricting and controlling remote network access and requiring the use of VPN with two-factor authentication; (g) maintaining secure network connections through the utilization of industry accepted protocols and

configuration; and (h) using secure services, protocols and ports to connect to or interact with any environment that stores, processes or transmits Four Seasons Personal Data.

18) *Endpoint management*. Vendor represents, warrants and covenants, that throughout the Term, it will take the following measures to regulate protection of its network, systems, and applications, to mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably be detected, including without limitation that at a minimum, Vendor will deploy and maintain (so that all are up to date) the following security technologies: (a) encryption of hard disks on company assigned workstations; (b) MFA in accordance with the terms of this Agreement; (c) centrally managed anti-virus protection, including without limitation Endpoint Detection and Response solutions (**EDR**); (d) file integrity management solutions for workstations and servers; (e) Mobile Device Management (**MDM**) solutions; (f) egress Internet filtering solutions; (g) management and monitoring of all software to control authorized software installations; (h) Vendor supplied software updates as required from time to time to ensure that all applicable software updates are applied to Vendor's systems; (i) login ID and password controls are implemented to authenticate to systems; (j) periodic review of endpoint security logs; and (k) e-mails are automatically scanned by anti-virus and anti-spam software.

19) *Audit*. Notwithstanding any to the contrary in the Addendum, Vendor agrees to maintain an information security program for the Services that complies with the SSAE 18 standard, ISO/IEC 27001:2013 or other alternative standards that are substantially equivalent to these standards for the establishment, implementation, control and improvement of security standards. Certification/audit activities: (a) will be performed at least annually; (b) will be performed according to ISO/IEC 27001:2013, SSAE 18 standards or such other alternative standards that are substantially equivalent to SSAE 18, provided that the certification/audit includes the applicable controls of Vendor's relevant to security, availability, processing integrity, confidentiality and privacy and includes both a test of design and a test of effectiveness; (c) will be performed by independent third-party security professionals at Vendor's selection and expense; and (d) will result in the generation of an audit report, which will be deemed Vendor's Confidential Information. Following completion of the implementation of any applicable Services, and on an annual basis, Vendor will, at Property's request and at no charge, provide Property with copies of any routine Service Organization Control reports (**SOC Reports**) (or any successor reports thereto) that are both directly related to those Services provided hereunder for Property and already released to Vendor by the public accounting firm producing the report, including without limitation (i) SSAE18 / SOC1 Type II relating to the Services; and SSAE18 / SOC2 Type II relating to the Vendor technical team supporting the Services. SOC Reports are Vendor's Confidential Information and Property will not distribute or allow any third party (other than its independent auditors) to use any such report without the prior written consent of Vendor. Property will instruct its independent auditors or other approved third parties to keep such report confidential and Property will remain liable for any unauthorized disclosure of such report by its independent auditors or other approved third parties. Vendor shall maintain complete and accurate records relating to its data protection practices and the security of any of Property's Confidential Information, including any backup, disaster recovery, or other policies, practices or procedures relating to Property's Confidential Information and any other information relevant to its compliance with this Section.

Annex 1

Vendor and Property Responsibility PCI Data Security Standard Matrix

High Level Overview	PCI DSS Req. No.	Description	Vendor Responsibility	Property Responsibility	Special Notes
Build and Maintain a Secure Network and Systems	1	Install and maintain a firewall configuration to protect cardholder data	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
	2	Do not use Consultant-supplied defaults for system passwords and other security parameters	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
Protect Cardholder Data	3	Protect stored cardholder data	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
	4	Encrypt transmission of cardholder data across open, public networks	☒ **YES** ☐ **NO**	☐ **YES** ☒ **NO**	
Maintain a Vulnerability Management Program	5	Protect all systems against malware and regularly update anti-virus software or programs	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
	6	Develop and maintain secure systems and applications	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
Implement Strong Access Control Measures	7	Restrict access to cardholder data by business need to know	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
	8	Identify and authenticate access to system components	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
	9	Restrict physical access to cardholder data	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
Regularly Monitor and Test Networks	10	Track and monitor all access to network resources and cardholder data	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	
	11	Regularly test security systems and processes	☒ **YES**	☒ **YES**	

			☐ **NO**	☐ **NO**	
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel	☒ **YES** ☐ **NO**	☒ **YES** ☐ **NO**	