Data Protection Addendum (G2 as Controller)

This Data Processing Agreement ("**DPA**") forms an integral part of the agreement signed between the G2 entity which is a party to the principal agreement ("**Company**" and "**Agreement**" respectively) and its counter party ("**Partner**", each "**Party**", together "**Parties**").
If Partner Processes Personal Data, or if Partner has access to Personal Data in the course of its performance under the Agreement, Partner shall comply with the terms and conditions of this DPA as a "processor", including Appendix 1 and Appendix 2, which are attached herewith and incorporated herein by reference ("**Attachments**").

1. Definitions and Interpretation

1.1 In this DPA:

1.1.1 "**Affiliate**" means any person or entity directly or indirectly controlling, controlled by, or under common control with a Party. For the purpose of this definition, "control" (including, with correlative meanings, the terms "controlling", "controlled by" and "under common control with") means the power to manage or direct the affairs of the person or entity in question, whether by ownership of voting securities, by contract or otherwise.

1.1.2 "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

1.1.3 "**Data Protection Laws**" means, as applicable, any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**").

1.1.4 "**Data Subject**" means a data subject to whom Personal Data relates.

1.1.5 "**Personal Data**" means any personal data that is processed by a party under the Agreement in connection with its provision or use (as applicable) of the Services.

1.1.6 "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Personal Data breach will comprise a Security Incident

1.1.7 "**Special Categories of Data**" means personal data as defined under Article 9 of the GDPR.

1.1.8 "**Standard Contractual Clauses**" mean the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission Decision 2010/87: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

1.1.9 "**Terms Effective Date**" means the effective date of the Agreement.

1.1.10 The terms "**controller**", "**processing**" and "**processor**" as used in this have the meanings given in the GDPR.

1.1.11 Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:

2.1.1 Partner processes Personal Data that is made available by the Company in connection with the Agreement;
2.1.2 The Data Protection Laws applies to the processing of Personal Data.

3. Roles and Restrictions on Processing

4.1 If Partner has access to or otherwise Processes Personal Data pursuant to the Agreement, then Partner shall:

4.1.1 only Process the Personal Data in accordance with Company's documented instructions and on its behalf, and in accordance with the Agreement and this DPA and related Attachments, including where relevant with regards to the transfer of personal data outside the EEA or to an international organization;

4.1.2 take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process, Personal Data; ensure persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and ensure that such personnel are aware of their responsibilities under this DPA and any Data Protection Laws (or Partner's own written binding policies are at least as restrictive as this DPA);

4.1.3 promptly, and in any case within the period of time required in Data Protection Laws, assist Company as needed to cooperate with and respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information (including details of the services provided by Partner) related to Partner's Processing of Personal Data;

4.1.4 notify the Company without undue delay, and no later than twenty-four (24) hours, after becoming aware of a Security Incident;

4.1.5 provide full, reasonable cooperation and assistance to Company in:

4.1.5.1 upon receipt of: (a) requests from Data Subjects to exercise their rights under the Data Protection Laws in connection with Personal Data Processed under this DPA, including (without limitation) the right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or the right not to be subject to an automated individual decision making; and/or (b) any requests or inquiries from supervisory authorities, customers, or others, to provide information related to Partner's Processing of Personal Data under this DPA, shall: (i) direct such requests to Company without undue delay, and (ii) not respond or act upon such requests without prior written approval from Company; and (iii) promptly, and in any case within the period of time required in Data Protection Laws, provide full, reasonable cooperation and assistance to Company in responding to and exercising such requests, except that the foregoing shall not apply only and insofar as it conflicts with Data Protection Laws.

4.1.5.2 ensuring compliance with any notification obligations of personal data breach to the supervisory authority and communication obligations to data subjects, as required under Data Protection Laws;

4.1.5.3 ensuring compliance with its obligation to carry out data protection impact assessments with respect to the Processing of Personal Data, and with its prior consultation with the supervisory authority obligation (as applicable).

4.1.6 only process or use Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;

4.1.7 as required under Data Protection Laws, maintain accurate written records of any and all the Processing activities of any Personal Data carried out under the Agreement (including the categories of Processing carried out and, where applicable, the transfers of Personal Data), and shall make such records available to the applicable supervisory authority on request;

4.1.8 make all reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Partner has the ability to do so;

4.1.9 upon termination of the Agreement, or upon Company's written request at any time during the term of the Agreement, Partner shall cease to Process any Personal Data received from Company, and within a reasonable period will at the request of Company: (1) return the

Personal Data; or 2) securely and completely destroy or erase all Personal Data in its possession or control (including any copies thereof), unless and solely to the extent the foregoing conflicts with any applicable laws. At Company's request, Partner shall give Company a certificate confirming that it has fully complied with this clause.

4. Subcontracting

4.1 Partner shall not subcontract its obligations under this DPA to another person or entity ("**Contractor(s)**"), in whole or in part, without Company's prior written approval or general written authorization, and shall inform the Company of any intended changes concerning the addition/replacement of other processors, no later than thirty (30) days prior to such intended change. Company shall have the right to object to the appointment of any new Contractor within 14 days of having been notified of the Contractor's appointment by Partner, in which event the Parties shall negotiate in good faith this objection. In the event the Parties, acting reasonably and in good faith, have not reached an amicable solution, then Company may terminate the portion of the Agreement that requires the employment of said Contractor.

4.2 Partner will execute a written agreement with such approved Contractor containing equivalent terms to this DPA and the applicable Attachments (provided that Partner shall not be entitled to permit the Contractor to further sub-contract or otherwise delegate all or any part of the Contractor's processing without Company's prior written consent at Company's sole discretion) and which expressly provides Company with third party beneficiary rights to enforce such terms and/or require Partner to procure that the Contractor enters into a Data Protection agreement with Company directly.

4.3 Company may require Partner to provide Company with full details of the proposed Contractor's involvement including but not limited to the identity of the Contractor, its data security record, the location of its processing facilities and a description of the access to Personal Data proposed.

4.4 Partner shall be liable for the acts or omissions of Contractors to the same extent it is liable for its own actions or omissions under this DPA.

5. Transfer of Personal Data

5.1 To the extent that Partner processes Personal Data outside the EEA, then the Parties shall be deemed to enter into the Standard Contractual Clauses, in which event: (i) the Standard Contractual Clauses are incorporated herein by reference, including the Attachments; and (ii) the Company shall be deemed as the data exporter and the Partner shall be deemed as the data importer (as these terms are defined therein).

5.2 Partner may process transfer Personal Data of outside the EEA ("**Transfer**"), only: (A) subject to the Company's prior written authorization, and (B) provided that the Transfer is necessary for the purpose of Partner carrying out its obligations under the Agreement or is required under applicable laws, and (C) provided the Transfer is done: (i) to an Approved Jurisdiction, or (ii) subject to the Standard Contractual Clauses, or through Privacy Shield framework as referred to in the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, or other applicable frameworks).

5.3 If Partner and/or Partner's Affiliates and/or their subcontractors intend to rely on Standard Contractual Clauses (where subcontracting or performance is allowed by the Agreement), then if the Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this DPA, and Partner will promptly begin complying with such Standard Contractual Clauses. Partner will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or sub-processor as the case may be.

6. Security Standards

6.1 Partner shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed; all other unlawful forms of Processing; including (as appropriate): (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

6.2 To the extent that Partner Processes Special Categories of Data, the security measures referred to in this DPA shall also include, at a minimum (i) routine risk assessments of Partner's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while "at rest" and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone).

7. General

7.1 If this DPA does not specifically address a particular data security or privacy standard or obligation, Partner will use appropriate, generally accepted practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

7.2 If Partner is unable to provide the level of protection as required herein, Partner shall immediately notify Company and cease processing. Any non-compliance with the requirements herein shall be deemed a material breach of the Agreement and Company shall have the right to terminate the Agreement immediately without penalty.

7.3 Company shall have the right to: (a) require promptly from Partner all information necessary to, and (b) conduct its own audit and/or inspections of Partner (including its facilities or equipment involved in the Processing of Personal Data) in order to: demonstrate compliance with the DPA and the applicable Attachments and/or Data Protection Laws. The Partner shall allow and contribute to such audit and/or inspection. Such audit and/or inspection shall be conducted with reasonable advanced notice to Partner and shall take place during normal business hours to reasonably limit any disruption to Partner's business.

7.4 Partner will indemnify Company other and hold Company harmless from any cost, charge, damages, expense or loss incurred as a result of Partner's breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon the party to be indemnified (the "**indemnified party**") promptly notifying the other party (the "**indemnifying party**") of a claim, (b) the indemnifying party having sole control of the defense and settlement of any such claim, and (c) the indemnified party providing reasonable cooperation and assistance to the indemnifying party in defense of such claim

8. Priority

8.1 If there is any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement then, the terms of this DPA will govern. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

9. Changes to this DPA

9.1 Company may change this DPA if the change is required to comply with Data Protection Laws, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the parties as independent controllers of Personal Data under the Data Protection Laws; (ii) expand the scope of, or remove any

restrictions on, either party's rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Partner, as reasonably determined by Company.

9.2 **Notification of Changes**. If Company intends to change this DPA under this Section, and such change will have a material adverse impact on Partner, as reasonably determined by Company, then Company will use commercially reasonable efforts to inform Partner at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

9.3 If any of the Data Protection Laws are superseded by new or modified Data Protection Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Data Protection Laws shall be deemed to be incorporated into this DPA, and each Party will promptly begin complying with such Data Protection Laws in respect of its respective processing activities.

APPENDIX 1

This Appendix 1 must be completed and signed by the parties. Except where explicitly stated otherwise, this Appendix is completed in accordance with Clause 2 of the Standard Contractual Clauses and forms an integral part of the Standard Contractual Clauses.

Details of Data exporter (Company)
the Data Exporter is the G2 entity which is a party to the Agreement

Details of Data importer (Partner)
The Data Importer is the Partner

Governing law
With reference to Clause 9 and Clause 11(3) of the Standard Contractual Clauses, the Standard Contractual Clauses shall govern by the law of the Member State in which the data exporter is established.

Data exporter and data importer activities relevant to the transfer
Activities relevant to the transfer include the performance of the Services for Company and customers, as contemplated in the Agreement.

Duration of the data processing
The duration of the data processing shall be the duration of the Agreement.

Data subjects
The personal data transferred may concern the following categories of data subjects:

- Data exporter's clients' end users

Categories of data
The personal data transferred may concern the following categories of data:

- Profile data (name, age, gender, physical address, telephone number, email address)
- Financial and payment data (e.g. credit card number, transactions and past transactions)
- Governmental IDs (passport copy or driver's license)

Special categories of data (if applicable)
The personal data transferred concern the following special categories of data:

- Health data

Purpose of processing operations
The transfer of personal data is made for the following purposes and subject to the below processing activities, as may be further set forth in contractual agreements entered into from time to time between the Company and Partner:

- Booking and reserving various services related to travel, accommodation and attractions

APPENDIX 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(c), 4(d) and 5(c) of the Standard Contractual Clauses.

Security Management

Partner maintains a written information security management system (ISMS), in accordance with this Appendix, that includes policies, processes, enforcement and controls governing all storage/processing/transmitting of Personal Data, designed to (a) secure Personal Data against accidental or unlawful loss, access or disclosure; (b) identify reasonable foreseeable and internal risks to security and authorized access to Partner Network, and (c) minimize security risks, including through risk assessment and regular testing. The information security program will include the following measures:

Partner actively follows information security trends and developments as well as legal developments with regards to the services provided and especially with regards to Personal Data and uses such insights to maintain its ISMS, as appropriate.

To the extent Partner process cardholder or payment data (such as payment or credit cards), Partner will maintain its ISMS in accordance with the PCI DSS standard, augmented to cover Personal Data, or such other alternative standards that are substantially equivalent to PCI DSS for the establishment, implementation, and control of its ISMS. Additionally, Partner will be assessed against PCI DSS annually by an on-site assessment carried out by an independent QSA (Qualified Security Assessor) and upon Company's request, not to exceed once annually, Partner will provide customer with PCI DSS Attestation of Compliance.

Maintain an Information Security Policy

Partner's ISMS is based on its security policies that are regularly reviewed (at least yearly) and maintained and disseminated to all relevant parties, including all personnel. Security policies and derived procedures clearly define information security responsibilities including responsibilities for:

- Maintaining security policies and procedures,
- Secure development, operation and maintenance of software and systems,
- Security alert handling,
- Security incident response and escalation procedures,
- User account administration,
- Monitoring and control of all systems as well as access to Personal Data.

Personnel is screened prior to hire and trained (and tested) through a formal security awareness program upon hire and annually. For service providers with whom Personal Data is shared or that could affect the security of Personal Data a process has been set up that includes initial due diligence prior to engagement and regular (typically yearly) monitoring.

Personal Data has implemented a risk-assessment process that is based on ISO 27005.

Secure Networks and Systems

Partner has installed and maintains a firewall configuration to protect Personal Data that controls all traffic allowed between Partner's (internal) network and untrusted (external) networks, as well as traffic into and out of more sensitive areas within its internal network. This includes current documentation, change control and regular reviews.

Partner does not use vendor-supplied defaults for system passwords and other security parameters on any systems and has developed configuration standards for all system components consistent with industry-accepted system hardening standards.

Protection of Personal Data

Partner keeps Personal Data storage to a minimum and implements data retention and disposal policies to limit data storage to that which is necessary, in accordance with the needs of its customers.
Partner uses strong encryption and hashing for Personal Data anywhere it is stored. Partner has documented and implemented all necessary procedures to protect (cryptographic) keys used to secure stored Personal Data against disclosure and misuse. All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.

Vulnerability Management Program

Partner protects all systems against malware and regularly updates anti-virus software or programs to protect against malware – including viruses, worms, and Trojans. Anti-virus software is used on all systems commonly affected by malware to protect such systems from current and evolving malicious software threats.
Partner develops and maintains secure systems and applications by:

- Having established and evolving a process to identify and fix (e.g. through patching) security vulnerabilities, that ensures that all systems components and software are protected from known vulnerabilities,
- Developing internal and external software applications, including web-applications, securely using a secure software development process based on best practices, e.g. such as code reviews and OWASP secure coding practices, that incorporates information security throughout the software-development lifecycle,
- Implementing a stringent change management process and procedures for all changes to system components that include strict separation of development and test environments from production environments and prevents the use of production data for testing or development.

Implementation of Strong Access Control Measures

"**Partner Network**" means the Partner's data center facilities, servers, networking equipment, and host software systems (e.g. virtual firewalls) as employed by the Partner to process or store Personal Data.
The Partner Network will be accessible to employees, contractors and any other person as necessary to provide the services to the Company. Partner will maintain access controls and policies to manage what access is allowed to the Partner Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Partner will maintain corrective action and incident response plans to respond to potential security threats.

Partner strictly restricts access to Personal Data by business need to know to ensure that critical data can only be accessed by authorized personnel. This is achieved by:

- Limiting access to system components and Personal Data to only those individuals whose job requires such access and
- Establishing and maintaining an access control system for systems components that restricts access based on a user's need to know, with a default "deny-all" setting.

Partner identifies and authenticates access to all systems components by assigning a unique identification to each person with access. This ensures that each individual is uniquely accountable for their actions and any actions taken on critical data and systems can be traced to known and authorized users and processes. Necessary processes to ensure proper user identification management, including control of addition/deletion/modification/revocation/disabling of IDs and/or credentials as well as lock out of users after repeated failed access attempts and timely termination of idling session, have been implemented.

User authentication utilizes at least passwords that have to meet complexity rules, which need to be changed on a regular basis and which are cryptographically secured during transmission and storage on all system components. All individual non-console and administrative access and all remote access use multi-factor authentication.

Authentication policies and procedures are communicated to all users and group, shared or generic IDs/passwords are strictly prohibited.

Restriction of Physical Access to Personal Data

Any physical access to data or systems that house Personal Data are appropriately restricted using appropriate entry controls and procedures to distinguish between onsite personnel and visitors. Access to sensitive areas is controlled and includes processes for authorization based on job function and access revocation for personnel and visitors.

Media and backups are secured and (internal and external) distribution is strictly controlled. Media containing Personal Data no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.

Regular Monitoring and Testing of Networks

All access to network resources and Personal Data is tracked and monitored using centralized logging mechanisms that allow thorough tracking, alerting, and analysis on a regular basis (at least daily) as well as when something does go wrong. All systems are provided with correct and consistent time and audit trails are secured and protected, including file-integrity monitoring to prevent change of existing log data and/or generate alerts in case. Audit trails for critical systems are kept for a year.

Security of systems and processes is regularly tested, at least yearly. This is to ensure that security controls for system components, processes and custom software continue to reflect a changing environment. Security testing includes:

- Processes to test rogue wireless access points,
- Internal and external network vulnerability tests that are carried out at least quarterly. An external, qualified party carries out the external network vulnerability tests.
- External and internal penetration tests using Partner's penetration test methodology that is based on industry-accepted penetration testing approaches that cover the all relevant systems and include application-layer as well as network-layer tests

All test results are kept on record and any findings are remediated in a timely manner.

Partner does not allow penetration tests carried out by or on behalf of its customers.

In daily operations IDS (intrusion detection system) is used to detect and alert on intrusions into the network and file-integrity monitoring has been deployed to alert personnel to unauthorized modification of critical systems.

Incident Management

Partner has implemented and maintains an incident response plan and is prepared to respond immediately to a system breach. Incident management includes:

- Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of customers,
- Specific incident response procedures,
- Analysis of legal requirements for reporting compromises,
- Coverage of all critical system components,
- Regular review and testing of the plan,
- Incident management personnel that is available 24/7,
- Training of staff,
- Inclusion of alerts from all security monitoring systems,
- Modification and evolution of the plan according to lessons learned and to incorporate industry developments.

Partner has also implemented a business continuity process (BCP) and a disaster recovery process (DRP) that is maintained and regularly tested. Data backup processes have been implemented and are tested regularly.

Physical Security

Physical Access Controls. Physical components of the Partner Network are housed in nondescript facilities ("Facilities"). Physical barrier controls are used to prevent unauthorized entrance to Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

Limited Employee and Contractor Access

Partner provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Partner of its affiliates.

Physical Security Protections

All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Partner also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, etc.) with door contacts, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

Continued Evaluation

Partner will conduct periodic reviews of the Security of its Partner Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Partner will continually evaluate the security of its Partner Network to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.