DATA PROCESSING AGREEMENT

This Data Processing Agreement including its annexes and the Standard Contractual Clauses referenced herein ("DPA") is made by and between Blueground (“Blueground”), and Customer, pursuant to the Agreement for the provision of services by Blueground as described in detail in the Agreement **(“Services”)** or any other written or electronic agreement between the parties ("**Agreement**"). This DPA is incorporated into the Agreement and governs the processing of Personal Data by Blueground under the Agreement. Its purpose is to ensure that such processing complies with applicable law and upholds the rights and freedoms of the individuals whose Personal Data is involved.

1. Definitions and Interpretation

1.1 All capitalised terms not defined herein shall have the meaning ascribed to them in the main body of the Agreement.

1.2 In the event of any conflict between the provisions of this DPA and those of the Agreement, the provisions of this DPA shall take precedence.

1.3 In this DPA:

“Account Data” means Personal Data that relates to Customer’s relationship with Blueground. This includes: (i) business contact details of Customer’s personnel (employees, agents and subcontractors); (ii) records of the communications between Blueground’s personnel representatives and Customer’s personnel or Clients (if applicable); (iii) keeping records of the services provided to the Customer or to its Clients; (iv) data provided by Clients directly to Blueground when they enter into a direct contract with it for the provision of its services; and (v) personal data Blueground must process as a controller to comply with applicable laws.

“**Affiliates**” means any entity which is in direct or indirect relation to a substantial administrative or financial dependence or control, in particular because of one’s participation in the other’s capital or administration or by the participation of the same persons in the capital or in the management of both companies.

“Anonymized” or “Anonymization shall mean the process in which personal data is transformed into information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information (a) take reasonable measures to ensure that the information cannot be associated with a consumer or household; (b) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this definition; (c) contractually obligates any recipients of the information to comply with this definition;

“**Applicable Data Protection Laws**” refers to laws and regulations applicable to Blueground’s processing of personal data under the Agreement, including but not limited to: all state, federal, or international laws, statutes, regulations, rules, treaties, executive orders, directives, or other official guidance or releases, and any industry rules or self-regulatory codes of conduct relating to data protection, privacy, data security, electronic communications, or Personal Data Breach that are then in effect and applicable to a party or Personal Data Processed under the Agreement. Data Protection Laws may include, without limitation: Regulation 2016/679 (“**GDPR**”), Directive 2002/58/EC (the “**ePrivacy Directive**”), and any laws, regulations, or rules implementing the

foregoing, or implemented in European Union Member States thereunder, and any successor directives or regulations thereof then in effect. Further, the UK Data Protection Act 2018, the UK GDPR (as defined in the Data Protection Act 2018), the UK Privacy in Electronic Communications (EC Directive) Regulations 2003; the Swiss Data Protection Act 2020; and the CCPA and CPRA;

"**Blueground**" means the Blueground entity with which the Customer is contracting based on an Agreement for the provision of Services.

"**CCPA**" means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder, in each case, as may be amended from time to time.

"**CPRA**" means the California Privacy Rights Act of 2020.

"Customer" means a party that has engaged Blueground for the provision of the Services.

"Customer's Client" means a physical or legal entity that has engaged the Customer for the provision of services.

"Customer's End Client" or "End Client" means the physical person(s) to whom Blueground's accommodation services are ultimately provided by virtue of an Agreement with Customer.

"**Customer Personal Data**" any personal data that Blueground processes on behalf of the Customer as a Data Processor and/or any of its End Clients as a Sub-Processor in connection with this DPA;

"**Data Processing Description Annex**" means Annex I;

"**Data Security Annex**" means Annex II;

"**EU GDPR**" means the General Data Protection Regulation ((EU) 2016/679), as it has effect in EU law;

"**IDTA Addendum**" means the UK Information Commissioner's Office (the "**ICO**") International Data Transfer Addendum to the EU Commission Standard Contractual Clauses;

"**Non-Adequate Country**" means any country or territory deemed to not have a data protection level "essentially equivalent" to the Applicable Data Protection Laws, as established in an adequacy decision;

"**Personal Data Breach**" any unauthorized destruction, loss, alteration, disclosure, acquisition or use of, or access to, personal data transmitted, stored or otherwise processed under this DPA, and any other event that may require Customer to provide notice to data subjects or regulatory authorities under Applicable Data Protection Laws;

"Privacy Policy" means the current privacy policy for the Services available at https://www.theblueground.com/privacy.

"**Recipient**" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not, or as otherwise defined in the Applicable Data Protection Laws;

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the EEA

to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"**Sub-Processor**" means a third-party who processes individuals' personal data on behalf of the Data Processor. Blueground may act as a Sub-Processor when Blueground processes Customer Personal Data and Customer is itself a Processor of such Customer Personal Data.

"**Standard Contractual Clauses (SCCs)**" means:

i. where the data exporter is established in the EU, and the EU Data Protection Legislation applies to the Processing prior to Transfer, the standard contractual clauses approved for the transfer of personal data to third countries, as adopted pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN (the "**EU SCCs**");

ii. where the data exporter is established in the UK, and where UK Data Protection Legislation applies to the Processing prior to a Transfer, the IDTA Addendum issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein ("**UK SCCs**");

iii. where the data exporter is established in Switzerland, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "**Swiss SCCs**")

iv. where the data exporter is established in Brazil, the Brazilian Data Protection Authority's standard contractual clauses for international data transfers pursuant to Law No. 13,709 as set out in Annex II of Resolution CD / ANPD No. 19, available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf (or a successor location) ("**Brazil SCCs**").

v. where the personal data of the exporter are subject to the LATAM and Canada Data Protection Requirements the Ibero-American Data Protection Network's model contractual clauses for international data transfers, as published by the Ibero-American Data Protection Network, available at https://www.redipd.org/en/document/annex-model-contractual-clauses-en.pdf (or a successor location) ("**LATAM and Canada SCCs**").

vi. where the data exporter is established in the KSA, the standard contractual clauses for personal data transfer approved by the Saudi Data and Artificial Intelligence Authority pursuant to the Regulation on Personal Data Transfer Outside the Kingdom under the PDPL, the Implementing Regulation of the PDPL and the Regulation on the Transfer of Personal Data Outside the Kingdom, available at https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf (or a successor location) ("**KSA SCCs**").

vii. where the data exporter is established in Türkiye, the standard contracts approved by the Personal Data Protection Board of Türkiye with its decision dated June 4, 2024 and numbered 2024/959, available at https://kvkk.gov.tr/Icerik/7938/Standart-Sozlesmeler-ve-Baglayici-Sirket-Kurallarina-Iliskin-Dokumanlar-Hakkinda-Kamuoyu-Duyurusu (or a successor location) ("**Türkiye SCCs**").

"**UK Transfers**" Transfers subject to and restricted by UK Data Protection Legislation.

For the purposes of this DPA, the terms **Controller**, **Processor**, **Data Subject**, **Personal Data**, **Processing** shall have the meaning given to them in the Applicable Data Protection Laws.

2. Scope and roles of the Parties

2.1 The provision of the Services as set forth in the Agreement requires the collection and processing of Customer Personal Data by the Data Processor. Where said processing is undertaken on behalf and under the direction of the Customer under Applicable Data Protection Laws, Customer shall be the Controller of the Customer Personal Data and Blueground the Data Processor. Where Customer is the Data Processor of Customer's Client and is engaging Blueground for the provision of the Services to said Customer's Client, Customer shall be the Processor of the Customer' Personal Data and Blueground the Sub-Processor.

2.2 Blueground shall act as a Controller in relation to the processing of Account Data. When acting as a Controller, Blueground shall be responsible for its compliance with Applicable Data Protection Laws, including without limitation ensuring a legal basis for the processing of such personal data. Customer shall not be held responsible or liable for any uses of data conducted by Blueground when Blueground is acting as a Controller.

2.3 Should the scope of cooperation between the Parties change, they shall use all reasonable endeavors to promptly make any changes that are necessary to this DPA.

3. Data Processor's obligations

The Customer designates Blueground as its Processor for the processing of Customer Personal Data, solely (a) in accordance with the Customer's instructions as outlined in the Agreement, this DPA, and as required for the provision of the Services to the Customer (including the investigation of security incidents and the detection or prevention of misuse or abuse); (b) as necessary to comply with applicable laws, including Applicable Data Protection Legislation; and (c) for any other purposes expressly agreed in writing between the parties (together, the "**Permitted Purposes**"). In particular, Blueground as a Data Processor undertakes to:

3.1 process the Customer Personal Data only on the documented instructions of Customer, unless Blueground is required by applicable laws to otherwise process that Customer Personal Data.

3.2 comply in the processing of Personal Data with its obligations under Applicable Data Protection Laws and the specific provisions established herein.

3.3 inform Customer if, in the opinion of Blueground, the instructions of Customer infringe Applicable Data Protection Laws;

3.4 not retain, use or disclose any Personal Data for any purpose other than the direct business relationship between the parties;

3.5 not sell (as defined under Applicable Data Protection Laws), share (as defined in the CCPA), or process Personal Data for any targeted or behavioral advertising, or other commercial purposes.

3.6 not combine Personal Data received from or processed on behalf of Customer with Personal Data it receives from or on behalf of third parties, except that Blueground may combine Personal Data (i) to provide its Services to the Customer, or (ii) as expressly permitted by Applicable Data Protection Laws.

3.7 implement and maintain appropriate technical and organisational measures, to protect Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. Blueground's security program shall be documented in writing, and in all material respects, meet the requirements of a recognized, industry-standard information security audit or certification standard. These measures shall be appropriate to the harm that might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of Customer Personal Data and having regard to the nature of Customer's Personal Data which is to be protected;

3.8 assist Customer and Customer's Clients at Data Controller's written request, without undue delay: (i) in responding to any request from a data subject; and (ii) to ensure Customer and its relevant Clients comply with their obligations under Applicable Data Protection Laws including without limitation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

3.9 at the Customer's reasonable request, provide assistance in the assessment and implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data;

3.10 ensure that the Customer Personal Data entrusted to it is not used for other purposes or processed in any other way than as stated in this DPA;

3.11 if it receives any complaint, notice or communication which relates directly or indirectly to the processing of the Customer Personal Data or to either party's compliance with any data protection laws, immediately notify Customer and provide Customer with full cooperation and assistance in relation to any such complaint, notice or communication;

3.12 reasonably cooperate with the Customer in the completion of any of Customer's cybersecurity audit, including by making available to the Customer, all relevant information that the auditor requests as necessary for the auditor to complete the Customer's cybersecurity audit;

3.13 reasonably cooperate with the Customer in conducting the Customer's risk assessment, including by making available to the business all facts necessary to conduct the risk assessment and not misrepresenting in any manner any fact necessary to conduct the risk assessment.

4. Customer's obligations

Customer undertakes to:

4.1. comply with its obligations under Applicable Data Protection Laws and the specific provisions established herein.

4.2. transmit, or in any way disclose to the Processor, only Personal Data which are strictly

necessary for the performance of the Services.

4.3. ensure the accuracy, quality and legality of the Customer's Personal Data and the means by which it has obtained such Data, including, in particular, where so required, obtaining consent from the Data Subjects, for the collection and processing of their Data.

4.4. ensure that its instructions for the processing of Personal Data are clear and comply with applicable Data Protection Laws and Regulations. Customer acknowledges that Blueground is neither responsible for determining which laws are applicable to Customer's business nor whether Blueground's Services meet or will meet the requirements of such laws. Customer will ensure that Blueground's processing of Customer Personal Data, when done in accordance with Customer's instructions, will not cause Blueground to violate any applicable law, including Applicable Data Protection Laws.

5. Description of processing

A detailed description of the processing activities undertaken by virtue of the Agreement is contained in Annex I hereof which forms an integral part of this DPA.

6. Compliance.

Blueground will comply with all Applicable Data Protection Laws, as well as all other laws, rules, and regulations applicable to Data Processor's Processing of Personal Data. Customer has the right to take reasonable and appropriate steps to ensure that Data Processor processes the Personal Data in a manner consistent with Customer's obligations under Applicable Data Protection Law, and, following notice to Data Processor, to stop and remediate unauthorized use of Personal Data.

7. Audits

7.1 The parties acknowledge that when Blueground is acting as a Processor on behalf of Customer, Customer must be able to assess Blueground's compliance with its obligations under Applicable Data Protection Laws and this DPA. To ensure that, Blueground's records of compliance and relevant documentation shall be open for inspection, examination, audit and copying by Customer or its designated agent(s) at all reasonable times, with reasonable prior written notice.

7.2 Upon reasonable written notice, Customer may require a third-party audit or security testing to evaluate Data Processor's compliance with its obligations under this DPA, including without limitation, relevant technical and organizational security measures. Such third party shall be selected by Customer in its sole discretion and at Customer's cost and expense. Any such audit shall be subject to Blueground's security and confidentiality terms and guidelines, may only be performed a maximum of once annually and will be restricted to only data relevant to Customer. Where the Auditor is a third-party, Blueground may object in writing to such Auditor, if in Blueground's reasonable opinion, the Auditor is not suitably qualified or provides services competitive to those of Blueground.

7.3 If any audit determines Blueground is in breach of this DPA, Blueground shall use commercially reasonable efforts to cure such breach within fourteen (14) days. Thereafter, provided that Blueground has failed to remedy such breach, Customer shall have the right, notwithstanding anything to the contrary in the DPA and Agreement, to terminate this DPA and Agreement.

8. Sub-processors

8.1. Customer provides a general authorization for Blueground to engage Sub-processors to undertake the processing of personal data under its directions and such Sub-processors respectively may engage third party processors to process Customer Personal Data on Blueground's behalf, provided that the following conditions are cumulatively met:

(a) Blueground will restrict the sub-processor's access to Customer Personal Data only to what is strictly necessary to provide the Services and in accordance with the Agreement, and Blueground will prohibit the Sub-processor from processing the Customer Personal Data for any other purpose.

(b) Blueground will impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data on any sub-processor it appoints that require such sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Legislation; and

(c) Blueground will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.

8.2. The Parties acknowledge that Customer's prior express approval shall be deemed to have been granted in respect to Blueground's Affiliates and current Sub-processors as listed at https://docs.theblueground.com/docs/List-of-Sub-processors.pdf ("**List of Sub-processors**").

8.3. Blueground may, by giving reasonable notice to the Customer, add or replace Sub-processors to the List of Sub-processors. Blueground will notify Customer if it intends to add or replace Sub-processors from the List of Sub-processors at least fifteen (15) days prior to any such changes. To receive such notification, Customers must subscribe to Blueground's Sub-processor distribution list, which is available at https://promos.theblueground.com/subprocessor-registration/. If Customer objects to the appointment of a new Sub-processor within fifteen (15) days of receiving such notice, on reasonable grounds relating to the protection of the Customer Personal Data, then Blueground will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to reach a mutually acceptable resolution within a reasonable time thereafter, Customer is permitted to terminate the Agreement.

9. Duration

The personal data processing relates to the provision of the Services and shall continue for the duration of the Agreement. This DPA will remain in force until the later of (a) the termination or expiry of the Agreement, or (b) the return or deletion of Customer Personal Data in accordance with Section 10 and Annex I hereof.

10. Return and deletion of Personal Data

10.1. Blueground will process Account Data as long as required (a) to provide the Services to Customer; (b) for Blueground's lawful and legitimate business needs; or (c) in accordance with applicable law or regulation. Account Data will be stored in accordance with Blueground's Privacy Policy.

10.2. Blueground shall process Customer Personal Data only for as long as necessary to fulfill the purposes for which it was collected. This means that personal data are deleted or anonymized

as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless retention obligations continue to apply. Customer may at any time request from Blueground to receive information on the specific retention periods of any category of personal data processed.

10.3. Customer may at any time request to Blueground the deletion of Account Data and Customer Personal Data, and Blueground will delete said data as soon as reasonably practicable and within a maximum period of 30 days from Customer's written request.

10.4. Upon termination or expiry of the Agreement, if Customer does not request the deletion of Customer Personal Data, and whereas the retention of specific data is not otherwise required, Blueground will automatically delete it from its systems 180 days after the termination or expiration of the Agreement.

Blueground may retain personal data beyond the standard retention period in the following circumstances:

- Legal Obligations: Where laws or regulations in applicable jurisdictions mandate a longer retention period, Blueground will retain the data for the duration required by those laws.

- Judicial Proceedings: If the data is necessary for ongoing or potential judicial, administrative, or regulatory proceedings, the Data Processor will continue to retain the data until the matter is fully resolved, including any applicable appeal periods.

- Preservation of Evidence: In cases of a legal claim or dispute, personal data relevant to the matter may be retained until the litigation or dispute is fully mitigated.

- Regulatory Investigations: Personal data may also be retained as required by regulatory bodies during investigations or audits

10.5. In case Blueground is required by applicable law to continue to store all or part of Customer Personal Data for a certain period ("**Regulatory Retention Period**"), Blueground shall delete such data immediately after the Regulatory Retention Period expires and certify its deletion to Customer at its request. For the purposes of this clause, Customer Personal Data shall be considered deleted where they are put beyond further use by Data Processor and are erased or irreversibly anonymized from Data Processor's and its Sub-processors' systems. To the extent applicable, Blueground represents and warrants that Data Processor shall make no attempt to re-identify any Anonymized Personal Data. Notwithstanding the foregoing, Data Processor agrees that any Anonymization conducted shall meet industry standards and shall be supported by sufficient technical and organizational measures to ensure re-identification cannot be conducted and that the data shall remain in anonymized form.

11. Technical and organizational measures

11.1. Blueground shall implement and safeguard the Customer Personal Data with the necessary technical and organizational measures appropriate to protect them against accidental or unlawful destruction or accidental loss, alterations, unauthorized disclosure or access. These measures shall at a minimum comply with the Applicable Data Protection Law and include the measures identified in Annex 2 (Technical and Organizational Security Measures).

11.2. Protective measures include using state-of-the-art software, computers, and encryption methods as well as the use of adequate access controls, password procedures, automatic blocking, case specific authorization concepts, logging and documentation of processes and the

implementation of a data security concept. The measures taken shall be adequate for the protection of the specific data, and protect against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in breach of Applicable Data Protection Laws. Blueground shall only allow access to Customer Personal Data on a need-to-know basis to employees who were informed about all relevant data privacy obligations. Employees shall be sufficiently trained in order to be able to comply with their data protection and contractual obligations. Blueground shall ensure an adequate level of training by implementing suitable controls;

11.3. Should the Customer reasonably find that Blueground's technical and organisational measures are inappropriate or ineffective, the Data Controller may request the undertaking of additional reasonable measures by the Data Processor to ensure its compliance with the Applicable Data Protection Laws.

12. Data subject rights

12.1. Blueground shall provide reasonable assistance to Customer in fulfilling its obligations regarding the exercise of Data Subjects' rights, as provided for in the Applicable Data Protection Laws.

12.2. Customer shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Customer Personal Data. If a Data Subject of Customer Personal Data submits a request directly to Blueground to exercise any of their rights under the Applicable Data Protection Laws concerning the personal data processed by the Data Processor pursuant to this agreement, and Blueground is able to through reasonable means, identify the Customer as the Controller of the Customer Personal Data of a Data Subject, Blueground shall, no later than 48 hours from receipt, forward this request to the Data Controller and accurately follow their instructions within the applicable deadline.

13. Data breach management

13.1. Blueground undertakes to inform the Customer of any Personal Data Breach incident affecting Customer Personal Data that comes to the attention of either Blueground or any of its Sub-processors.

13.2. The notification must occur immediately and without undue delay after becoming aware of the Personal Data Breach. Notwithstanding the foregoing, Blueground shall assist Customer with any updates or further information on Customer's reasonable request, and as required to fulfill the parties' obligations under Applicable Data Protection Law.

13.3. The information Blueground must provide to the Customer includes at least the following:

(a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of affected data subjects, and the categories and approximate volume of affected personal data;

(b) the name and contact details of the person managing the breach incident, if different from the data protection officer;

(c) a description of the possible consequences of the personal data breach;

(d) a description of the measures taken or proposed to address the personal data breach,

including, where appropriate, measures to mitigate possible adverse effects.

13.4. If it is not possible to provide all the information simultaneously, it can be provided gradually, without undue delay.

13.5. Blueground shall cooperate with the Customer and take all necessary actions to investigate, contain, remediate the cause, and mitigate any effects or potential harms to any data subjects arising from any actual or reasonably suspected Personal Data Breach and to promptly restore the security level of its systems.

14. Confidentiality

Parties represent that Customer Personal Data are considered Confidential Information. Therefore, Blueground undertakes to ensure that its personnel and officers involved in the collection and processing of Personal Data:

(a) are informed of the confidential nature of the Data.

(b) have received appropriate training on their responsibilities with regard to the protection of Personal Data.

(c) have signed confidentiality agreements or are under an appropriate legal obligation of confidentiality.

15. Transfer mechanism

15.1. Customer acknowledges that Blueground and its Sub-processors may transfer and process personal data to Non-Adequate Countries in which Blueground, its Affiliates or its Sub-processors maintain data processing operations, as more particularly described in the Sub-processor List. Blueground shall ensure that, when the transfer of personal data from Customer (as "data exporter") to Blueground (as "data importer") is a Restricted Transfer, appropriate safeguards are put in place. For the purposes of such Restricted Transfers, the Parties agree that the appropriate SCCs shall apply and are incorporated into this DPA by reference and deemed signed, as follows:

15.1.1. For the purposes of the EU SCCs, the following provisions shall be applicable:

A. In relation to transfers of **Customer Personal Data** that is protected by the GDPR, the EU SCCs shall apply, completed as follows:

- Module Two (in case Customer is Controller and exporter and Blueground is Processor and importer) or Module Three will apply (in case Customer is Processor and exporter and Blueground is (Sub)processor and importer);

- In Clause 7, the optional docking clause will apply;

- In Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in section 8.3 of this DPA;

- In Clause 17 (governing law) and 18 (forum and jurisdiction) the EU SCCs will be governed by the laws and competent courts of Greece.

- In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Greek law;

- Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and

- Subject to section 11 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA.

B. In relation to transfers of **Account Data** protected by the GDPR and processed in accordance with Section 2.2 of this DPA, the EU SCCs shall apply, completed as follows:

- Module One will apply;

- In Clause 7, the optional docking clause will apply;

- In Clause 11, the optional language will not apply;

- In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Greek law;

- In Clause 18(b), disputes shall be resolved before the courts of Greece;

- Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and

- Subject to section 11 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA;

15.1.2. For the purposes of the personal data protected by the **UK GDPR or the Swiss Legislation**, the following provisions shall be applicable:

- References to "Regulation (EU) 2016/679" shall be interpreted as references to UK Privacy Laws or the Swiss DPA (as applicable);

- References to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Privacy Laws or the Swiss DPA (as applicable);

- References to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);

- The term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);

- Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);

- References to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

- In Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and

- With respect to transfers to which UK Privacy Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

- For the purposes of the UK and Swiss SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Annexes 1 and 2 of this DPA.

- In relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows: (i) apply as completed in accordance with paragraph 15.1.2 above; and (ii) be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex I and Annex II of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

15.1.3. To the extent that Personal Data which is subject to **Brazil** Data Protection Requirements is transferred to Blueground in connection with the Agreement, such Processing shall be governed by the Brazil SCCs. For purposes of the Brazil SCCs:

- Where Blueground and Customer are Controllers, the Exporter and Designated Party shall be Customer and the Importer shall be Blueground;
- Where Blueground is a Controller and Customer is a Processor, the Exporter shall be Customer and the Importer and Designated Party shall be Blueground;
- Where Blueground is a Processor and Customer is a Processor, the Exporter shall be Customer and the Importer shall be Blueground and the applicable Controller and its contact details are as specified in the Agreement; and
- Where Blueground is a Processor and Customer is a Controller, the Exporter and Designated Party shall be Customer and the Importer shall be Blueground.
- Unless otherwise prohibited under the Agreement, Blueground is authorized to carry out Onward Transfers of Personal Data provided all provisions of Clause 18 of the Brazil SCCs as well as all applicable provisions of the Agreement are observed.
- Unless otherwise prohibited under the Agreement, Blueground is authorized to carry out Onward Transfers of Personal Data provided all provisions of Clause 18 of the Brazil SCCs as well as all applicable provisions of the Agreement are observed.
- For the purposes of the Brazil SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Annexes 1 and 2 of this DPA.

15.1.4. **Kingdom of Saudi Arabia** (“KSA”). To the extent that Personal Data which is subject to KSA Data Protection Requirements is transferred by Customer to Blueground in connection with the Agreement, such Processing shall be governed by the KSA SCCs. For purposes of the KSA SCCs:

- Where Blueground and Customer are Controllers, the Personal Data Exporter shall be Customer, the Personal Data Importer shall be Blueground, and the First Template (“Controller to Controller”) shall apply;
- Where Blueground is a Processor and Customer is a Controller, the Personal Data Exporter shall be Customer, the Personal Data Importer shall be Blueground, and the Second Template (“Controller to Processor”) shall apply;
- For the purposes of the KSA SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Annexes 1 and 2 of this DPA

15.1.5. **LATAM and Canada**. To the extent that Personal Data which is subject to LATAM and Canada Data Protection Requirements is transferred by Customer to Blueground in connection with the Agreement, such Processing shall be governed by the LATAM and Canada SCCs. For purposes of the LATAM and Canada SCCs:

- Where Blueground and Customer are Controllers, the Data Exporter shall be Customer, the Data Importer shall be Blueground, and the "Controller to Controller" clauses shall apply; and
- Where Blueground is a Processor and Customer is a Controller, the Data Exporter shall be Customer, the Data Importer shall be Blueground, and the "Controller to Processor" clauses shall apply. For Clause 7 in those clauses: Option 2 (general written authorization) is selected. Unless otherwise prohibited under the Agreement, Blueground is authorized to carry out Onward Transfers of Personal Data to the Sub-processors included in the Agreement in accordance with Clause 7.
- Competent Supervisory Authority: according to Applicable Law.
- For the purposes of the Brazil SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Annexes 1 and 2 of this DPA.

15.1.6**. Türkiye**. To the extent that Personal Data which is subject to Türkiye Data Protection Requirements is transferred by Customer to Blueground in connection with the Agreement, such Processing shall be governed by the Türkiye SCCs. For purposes of the Türkiye SCCs:

- Where Blueground and Customer are Controllers, the data exporter shall be Customer , the data importer shall be Blueground , and the "Data Controller to Data Controller" contract shall apply;
- Where Blueground is a Controller and Customer is a Processor, the data exporter shall be Customer, the data importer shall be Blueground, and the "Data Processor to Data Controller" contract shall apply;
- Where Blueground is a Processor and Customer is a Processor, the data exporter shall be Customer, the data importer shall be Blueground, and the "Data Processor to Data Processor" contract shall apply;
- Where Blueground is a Processor and Customer is a Controller, the data exporter shall be Customer, the data importer shall be Blueground, and the "Data Controller to Data Processor" contract shall apply.
- For the purposes of the Türkiye SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Annexes 1 and 2 of this DPA

15.2. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

16. No Sale of data

Where the processing of Customer Personal Data is governed by U.S. data protection laws, Blueground shall not: (a) sell Customer Personal Data or otherwise disclose it to any third party in exchange for monetary or other valuable consideration; (b) share Customer Personal Data with any third party for purposes of cross-context behavioral advertising; (c) retain, use, or disclose Customer Personal Data for any purpose other than the business purposes set forth in this DPA or as otherwise permitted under applicable U.S. data protection laws; (d) retain, use, or disclose Customer Personal Data outside the direct business relationship between the parties; or (e) combine Customer Personal

Data with personal data obtained from other sources or from its own interactions with the data subject, unless permitted under applicable U.S. data protection laws. Blueground shall promptly inform the Customer if it determines that it can no longer comply with its obligations under applicable U.S. data protection laws.

17. MISCELLANEOUS

17.1. Each Party warrants that it has the power and authority to enter into this DPA and perform its obligations hereunder.

17.2. This DPA constitutes and contains the entire agreement of the Parties with respect to the subject matter of this DPA, and supersedes any and all prior negotiations, correspondence, understandings and agreements regarding the subject matter of this DPA. Nothing in this DPA shall be read or construed as excluding any liability or remedy in respect of fraud.

17.3. If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. The order of precedence will be: (a) this DPA; (a) the Agreement; and (c) the Privacy Policy. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

17.4. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 2.2 hereof, Blueground reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation. Blueground will provide Customer with at least fifteen (15) days' notice of such amendments, during which time the Customer may reasonably object. The parties will work together in good faith to agree on any measures required to ensure compliance with the law.

17.5. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA.

17.6. This DPA and any dispute or claim (including non-contractual disputes or claims) 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 established in the Agreement. Each Party irrevocably agrees that any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this DPA or its subject matter or formation shall be resolved by the competent Courts provided in the Agreement. Where the E.U S.C.Cs or the IDTA Addendum are applicable, the Supervisory Authority, the governing law and the competent courts shall be established respectively in accordance with the Data Processing Description Annex and article 15 hereof.

ANNEX I

DATA PROCESSING DESCRIPTION

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter, including any contact person with responsibility for data protection]

Name	As established in the Agreement.
Contact person's name, position and contact details	As established in the Agreement.
Activities relevant to the data transferred under these Clauses	Receipt of the Services by the Data Importer
Role	Controller

Data importer(s): [Identity and contact details of the data importer, including any contact person with responsibility for data protection]

Name	The Blueground entity set forth in the Agreement
Contact person's name, position and contact details	Blueground's Data Protection Officer - dpo@theblueground.com
Activities relevant to the data transferred under these Clauses	Provision of the Services to the Data Exporter.
Role	Processor

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose personal data are transferred	**Module One** Customer's employees and individuals authorized by Customer to access Customer's Blueground account and/or cooperate with Blueground by virtue of the Agreement. **Modules Two and Three** End Clients to whom Blueground's accommodation Services are provided and (where applicable) their accompanying family members and emergency contacts.
Categories of personal data transferred	**Module One** Account Data which constitutes Personal Data, such as name and contact information (email, telephone number). **Modules Two and Three**

	Any Customer Personal Data processed by Blueground in connection with the Services requested by the Customer and which relate to the services ultimately provided to the End users. This includes but is not limited to: ● First and last Name ● Date of Birth ● Email ● Passport copy ● Host Location ● Booking details ● Passport Issue Date ● Nationality ● Passport Number ● Telephone number ● Passport Expiry Date ● Copy of driver's license ● Passport Issuing Place ● Driver's license number ● Social Security number
Transfers of Special Categories of Personal Data	Blueground does not knowingly collect or process any Special Categories of Personal Data within the meaning of the GDPR.
Frequency of the Transfer	**Module One** Continuous **Modules Two and Three** Intermittent: Data will be transferred where so required for the provision of the Services based on the Customer's requests.
Nature of the Processing	Collection, storage, and organization of personal data for the provision of the Services Access and retrieval of personal data for the provision of the Services. Updating and correcting personal data as needed. Deletion or anonymization of personal data when no longer required.
Purpose(s) of the data transfer and further processing	**Module One** Personal data contained in Account Data and will be processed in order to manage the account, including to access Customer's account, to maintain or improve the performance of the Services, to provide

	support, to investigate and prevent system abuse, or to fulfill legal obligations. **Modules Two and Three** To provide the Services in accordance with the Agreement and to comply with legal and regulatory requirements.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	**Module One** Blueground will process Account Data as long as required (a) to provide the Services to Customer; (b) for Blueground's lawful and legitimate business needs; or (c) in accordance with applicable law or regulation. Account Data will be stored in accordance with Blueground's Privacy Policy. **Modules Two and Three** Blueground shall process personal data only for as long as necessary to fulfill the purposes for which it was collected. This means that personal data are deleted or anonymized as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless retention obligations continue to apply. Customer may at any time request from Blueground to receive information on the specific retention periods of any category of personal data processed. Customer may at any time request to Blueground the deletion of Customer Personal Data, and Blueground, unless a legitimate purpose for their retention exists (e.g the continued provision of services to such End Client), will delete said data as soon as reasonably practicable and within a maximum period of 30 days from Customer's written request. Upon termination or expiry of the Agreement, if Customer does not request the deletion of Customer Personal Data, and whereas the retention of specific data is not otherwise required, Blueground will automatically delete it from its systems 180

	days after the termination or expiration of the Agreement. Blueground may retain personal data beyond the standard retention period in the following circumstances: ● Legal Obligations: Where laws or regulations in applicable jurisdictions mandate a longer retention period, Blueground will retain the data for the duration required by those laws. ● Judicial Proceedings: If the data is necessary for ongoing or potential judicial, administrative, or regulatory proceedings, the Data Processor will continue to retain the data until the matter is fully resolved, including any applicable appeal periods. ● Preservation of Evidence: In cases of a legal claim or dispute, personal data relevant to the matter may be retained until the litigation or dispute is fully mitigated. ● Regulatory Investigations: Personal data may also be retained as required by regulatory bodies during investigations or audits.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Blueground shall limit any sub-processor's access to Customer Personal Data strictly to the extent necessary for the provision of the Services and as permitted under the Agreement, and shall ensure that such sub-processor is prohibited from processing the data for any other purpose. Blueground shall impose written data protection obligations on each sub-processor, including requirements to implement appropriate technical and organizational measures, so that Customer Personal Data is safeguarded in accordance with Applicable Data Protection Legislation. Blueground shall remain fully liable and responsible for any breach of this DPA resulting from the acts or omissions of its sub-processors.

C. COMPETENT SUPERVISORY AUTHORITY

For the purpose of Clause 13 (supervision) in EU SCCs for International Transfers, the supervisory authority responsible for ensuring compliance, will be the Hellenic Data Protection Authority.

For the purpose of UK Transfers and the IDTA Addendum, the supervisory authority responsible for ensuring compliance, will be the UK Information Commissioner's Office.

For data transfers subject to the Swiss Federal Act on Data Protection, the competent supervisory authority under the Standard Contractual Clauses shall be the Federal Data Protection and Information Commissioner (FDPIC).

For the purposes of the Brazil, KSA, LATAM and Canada and Türkiye SCCs, the Competent Supervisory Authority shall be the respective Competent Authority of each jurisdiction in accordance with the applicable legislation.

ANNEX II

DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SECURITY MEASURES IMPLEMENTED BY BLUEGROUND IN ITS CAPACITY AS THE DATA IMPORTER

Where applicable, this ANNEX II will serve as Annex II to the Standard Contractual Clauses. The following provides more information regarding the technical and organizational security measures set forth below.

Confidentiality	**Physical access control** • Safety locks to get into the office. • Use of AWS cloud provider to store data. • Physical Environments monitored and supported with appropriate methods of detection and alerting. • Physical access to sensitive areas is secured to appropriate standards. **Logical access control** • Secure passwords including the use of strong passwords • Two-Factor authentication for all key systems. • Encryption of personal data whenever possible. **Data access control** ● Role based access control ● Need-based rights of access (only on a need-to-know basis). **Events Logging** • System time clocks are synchronized to trusted time sources. • Log records are created, protected and retained to the extent needed to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity. **Isolation and separation**

	• Client data is logically segregated from other clients' data. • Database rights are centrally managed and set as granular as possible. • Production data is not used in non-production environments **Encryption of personal data** Personal data encrypted by default, applied at rest and in transit across untrusted networks. **Security** • Blueground has implemented corporate information security practices and standards that are designed to safeguard the corporate environment and to address business objectives across information security, system and asset management, development, and governance. • These practices and standards are approved by Blueground executive management and are periodically reviewed and updated where necessary. • Blueground maintains appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. • Security policies are reviewed annually.
Integrity	**Data transmission and transport control** • Internet connectivity and email transmissions are secured with anti- malware detection. • Network segments are controlled by firewalls with monitoring and alerting. • Protections are on end-user devices and monitor those devices to be in compliance with the security standard requiring screen lock timeout, malware software, firewall software,

	remote administration, unauthenticated file sharing, hard disk encryption and appropriate patch levels. • Controls are implemented to detect and remediate workstation compliance deviations. • Blueground is using only secured connections (SSL/HTTPS with TLS1.2 and higher). • Encrypting all Data in transit and at rest. **Data during storage** • Mandatory application of encryption for data at rest. • Access control adheres to the principle of least privilege. • Data assets subject to backup and recovery processes. **Limited Data Retention** • Data retained no longer than required for the Blueground to comply with its obligations under the DPA and with local laws and subject to secure data destruction practices. **Security Incidents** In case of incident, Blueground will follow documented incident response procedures to comply with applicable laws and regulations.
Availability and resilience	**Availability control** • Backups are stored in a secured cloud storage with multi-location security. • Blueground is using AWS as a hosting provider. • Blueground has a recovery plan which is tested annually at least.

ANNEX III
List of Sub-Processors

In Clause 9 of the SCCs, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in art. 8 (Sub-processors) of this DPA. Customer agrees that (a) Blueground may engage Blueground affiliates and Sub-processors as listed at https://docs.thebluegroud.com/docs/List-of-Sub-processors.pdf (the "List of Sub-processors") and (b) Blueground may, by giving reasonable notice to the Customer, add or replace Sub-processors to the List of Sub-processors. Blueground will notify Customer if it intends to add or replace Sub-processors from the List of Sub-processors at least fifteen (15) days prior to any such changes. To receive such notification, Customers must register to Blueground's List of Sub-processors notification form, available at https://promos.thebluegroud.com/subprocessor-registration/. If Customer reasonably objects to the appointment of a new Sub-processor within fifteen (15) days of receiving such notice, on reasonable grounds relating to the protection of the Customer Personal Data, then Blueground will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to reach a mutually acceptable resolution within a reasonable time thereafter, Customer is permitted to terminate the Agreement.