Data Processing Addendum

This Data Processing Addendum including all attached Schedules ("**DPA**") forms part of the Agreement between: Ten Twenty Four, Inc. d/b/a Beyond Pricing **(**"**Service Provider**"**)**, acting on its behalf and/or agent for its Affiliates, and you (either a Subscriber or a User, each a "**Customer**").

The terms used in this DPA shall have the meanings set forth in this DPA. Except as modified below, the terms of the Agreement shall remain in full force and effect. All capitalized terms not defined herein will have the meaning set forth in the Agreement

The parties hereby agree that the terms and conditions set out below in this DPA shall be added as an addendum to the Agreement.

1. Definitions.

1.1. "**Applicable Laws**" means any privacy or security law that applies to Customer Personal Data, including the EU and UK General Data Protection Regulation ("**GDPR**") and US Data Protection Laws.

1.2. "**Controller**" means the natural or legal person or entity who determines the purposes and means of the Processing of the Customer Personal Data. Controller is also a "business," as that term is defined by US Data Protection Laws.

1.3. "**Customer Personal Data"** means information that is Processed by Service Provider and/or Customer, or collected by Service Provider and/or Customer, on behalf of Customer which identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular identified or identifiable person or household.

1.4. **"Data Subject"** means any identifiable individual or household included, or previously included, within the Customer Personal Data.

1.5. **"Process"** means any operation or set of operations that are performed on Customer Personal Data.

1.6. **"Processor"** means any entity that performs the Processing of Customer Personal Data. For the purposes of this Agreement and DPA, Service Provider and any authorized subcontractors are Processors.

1.7. **"Personal Data Breach"** means the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed. Should any other definition of "breach," "data breach," or "personal data breach" that appears in any Applicable Law be broader in scope than the definition provided here, the definition in said law shall control.

1.8. **"Regulator"** refers to any government agency responsible for enforcing the Applicable Laws.

1.9. "**Sell**"/"**Sale**" has the meaning as may be set forth in the US Data Protection Laws (e.g. the California Consumer Privacy Act of 2018). By example, and not by way of limitation, "Sell" may mean selling, renting, releasing, disclosing, disseminating, making available or transferring a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

1.10. "**Share**" has the meaning as may be set forth in US Data Protection Laws (e.g. the California Privacy Rights Act of 2020). By example, and not by way of limitation "Share" may mean any disclosure of Customer Personal Data (renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means) to a third parties for cross-contextual behavioural advertising.

1.11. "**Subprocessor**" means any Processor (including any third party and any Service Provider Affiliate) appointed by Service Provider to Process Customer Personal Data.

1.12. "**US Data Protection Laws**" means the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, the Connecticut Data Privacy Act, and any other United States state privacy legislation of similar scope to the aforementioned statutes that become enforceable after effective date of this DPA, and any implementing regulations adopted thereunder (all of which as may be amended from time to time).

2. **Authorization to Process Data.**

2.1. The parties acknowledge and agree Customer is a Controller, and Service Provider is a Processor with respect to Customer Personal Data. Service Provider may Process Customer Personal Data per the terms of the Agreement and this DPA with Customer. Customer represents and warrants that all Customer Personal Data provided to Service Provider by Customer does not violate the rights of Data Subjects or the Applicable Laws.

2.2. Service Provider and Customer each represents and warrants that it will comply with Applicable Laws. Service Provider will notify Customer if Service Provider makes a determination that it can no longer meet its obligations under the Applicable Laws.

2.3. Service Provider shall not Process Customer Personal Data for any purpose other than those specified in the Agreement, this DPA, and any instruction which Customer provides to Service Provider. Service Provider shall immediately inform the Customer if, in its opinion, any Processing instruction infringes upon any Applicable Law.

2.4. As part of Service Provider providing the Services to Customer, Customer agrees that Service Provider may: (a) de-identify or aggregate Customer Personal Data and (b) Process Customer Personal Data for purposes of identifying threats and malicious activity, mitigating fraud, financial loss or other harm; establishing, exercising, or defending legal claims; and maintaining and improving the quality of Service Provider's products, services, and systems.

2.5. Schedule 1 to this DPA sets out certain information regarding the Service Provider's Processing of the Customer Personal Data.

2.6. Each party represents and warrants it will comply with Applicable Laws, including all regulations that have been or are further enacted relating thereto, and other similar applicable privacy and data protection laws and regulations, including without limitation, addressing Data Subject requests as required by Applicable Laws.

3. **Processing Obligations & Restrictions**

3.1. Customer represents and warrants that it has all rights necessary to provide Customer Personal Data to Service Provider in connection with providing the Services. Any Customer Personal Data that Customer discloses to, transfers, or permits access by Service Provider in connection with the Services is disclosed, transferred, or permitted solely for the limited and specified business purpose(s) set forth in Schedule 1. Customer and Service Provider agree that any provision or transfer of Customer Personal Data by or on behalf of Customer to Service Provider under the Agreement is done in the context of Service Provider acting as a Processor/service provider and is not a Sale or Sharing of such data and shall not otherwise be for any monetary or other consideration. Further, no Customer Personal Data is shared for targeted or cross-contextual advertising purposes.

3.2. In the course of providing Services to Customer in connection with Customer Personal Data it receives, accesses, transfers, or collects in connection with the Services, Service Provider agrees that it will:

3.2.1. Process Customer Personal Data in accordance with the purpose, type, and categories of Customer Personal Data and Data Subjects as set out in Schedule 1;

3.2.2. Not access, retain, use, or disclose Customer Personal Data for any purpose other than as needed to perform the Services under the Agreement, as outlined in Schedule 1, or as otherwise permitted by Applicable Laws or other applicable law;

3.2.3. Not access, retain, use, or disclose Customer Personal Data for a commercial purpose other than as needed to perform the Services under the Agreement;

3.2.4. Not access, retain, use, or disclose Customer Personal Data outside of the direct business relationship between Service Provider and Customer other than as needed to perform the Services under the Agreement;

3.2.5. Not attempt to identify or re-identify any Data Subject and not associate any personal information with any Data Subject or any Data Subject's online activity, other than as strictly required to provide Services to Customer;

3.2.6. Not Sell, Share, or license to any third party, or use for the benefit of any third party, any Customer Personal Data;

3.2.7. Not co-mingle or combine Customer Personal Data with the data of any third party, other than as strictly required to perform the Services;

3.2.8. Notify Customer if it makes a determination that it can no longer meet its obligations under the Applicable Laws or other applicable law;

3.2.9. Permit Customer to take reasonable and appropriate steps to ensure Service Provider uses Customer Personal Data in a manner consistent with Applicable Laws;

3.2.10. Permit Customer to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data by Service Provider; and

3.2.11. Promptly notify Customer if, in Service Provider's reasonable opinion, any instruction or direction from the Customer infringes Applicable Laws;

3.3. Service Provider certifies that it understands and will comply with the restrictions on the use of Customer Personal Data in connection with providing the Services.

4. **Customer Obligations**. Customer shall, in its use of the Services, Process Customer Personal Data in accordance with the requirements of Applicable Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data.

5. **Confidentiality**. Service Provider shall take reasonable steps and adhere to industry standards to ensure the confidentiality of any employee, agent or contractor that has access to the Customer Personal Data. Among other things, Service Provider will limit access to those individuals who need to access Customer Personal Data and will ensure that any person authorized to Process Customer Personal Data shall be subject to a duty of confidentiality.

6. **Security**. Service Provider shall implement reasonable and appropriate industry standard technical and organizational measures to protect Customer Personal Data as described in Schedule 2 to this DPA.

7. **Subprocessing**.

7.1. Customer hereby grants general written authorization to Service Provider to appoint Subprocessors to perform specific Processing activities on its behalf. Service Provider's current Subprocessors are set forth at: www.beyondpricing.com/beyond-subprocessors. Service Provider will inform Customer of any intended changes concerning the addition or replacement of its Subprocessors and Customer will have an opportunity to object to such changes on objectively and reasonably justifiable grounds related to the inability of such Subprocessors to protect Customer Personal Data in accordance with the relevant obligations of this DPA or Applicable Laws, within ten (10) days after being notified. If the parties cannot resolve Customer's objection, Customer may cease using the Services and/or terminate the Agreement.

7.2. With respect to each Subprocessor, Service Provider shall:

7.2.1. include terms in the contract between Service Provider and each Subprocessor that are materially similar to the terms set out in this DPA; and

7.2.2. remain fully liable to Customer for the performance of such Subprocessors' obligations.

8. **Data Subject Rights**.

8.1. Service Provider shall assist Customer in responding to complaints, communications, or requests by a Data Subject to exercise a right under Applicable Laws relating to the Customer Personal Data.

8.2. Service Provider shall promptly notify Customer if it receives a request from a Data Subject in respect to Customer Personal Data, including a request by a Data Subject that Service Provider access, modify, or delete Customer Personal Data. Service Provider shall await instructions from Customer concerning whether, and how to respond to such a request.

8.3. With regard to Service Provider's obligations pursuant to Sections 8.1 and 8.2, (a) Service Provider will provide such assistance only to the extent that such assistance is strictly necessary for the fulfilment of Customer's obligations and relates to Service Provider's Processing of Customer Personal Data; and (b) Customer shall be responsible for any costs and expenses arising from Service Provider's obligations.

9. **Personal Data Breach**.

9.1. Service Provider shall notify Customer without undue delay of becoming aware of a Personal Data Breach upon Service Provider or any Subprocessor becoming aware of a Personal Data Breach potentially affecting Customer Personal Data and will provide Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or relevant Regulators of the Personal Data Breach.

9.2. Service Provider shall, and shall require any Subprocessor to, co-operate with Customer and take such reasonable commercial steps to assist in the investigation, mitigation, and remediation of any such Personal Data Breach.

10. **Data Protection Impact Assessments and Prior Consultation**. Service Provider shall provide reasonable assistance to Customer with any data protection impact assessments which are required under Applicable Law in relation to the Service Provider's Processing of Customer Personal Data.

11. **Deletion or return of Customer Personal Data**.

11.1. Subject to Section 11.2, upon (i) termination or expiration of the Agreement and (ii) deletion of Customer's account, or at any time upon your request, Service Provider will destroy (such that it is physically and logically irrecoverable) Customer Personal Data subject to Applicable Laws and in accordance with the Agreement and Service Provider's data retention policies. Alternatively and if required by Applicable Laws, upon Customer's request, Service Provider will return all Customer Personal Data to Customer. The Services allow Customer to retrieve Customer Personal Data at any time prior to deletion of Customer's account. Where Service Provider is to destroy Customer Personal Data, it shall do so once it is no longer needed to perform the Services. Upon termination or expiration of the Agreement, and where Service Provider is to return Customer Personal Data if required by Applicable Laws, Service Provider will then destroy any remnant copies of the Customer Personal Data that remain in its possession or under its control. Service Provider will ensure that any Customer Personal Data that is provided to any third party for purposes of performing the Services is likewise either returned to Customer and/or destroyed, as set forth in this Section 11.1.

11.2. Notwithstanding Section 11.1 of this DPA, Service Provider may retain Customer Personal Data (i) to the extent required or permitted by Applicable Laws and (ii) that Service Provider has archived to back-up systems ("**Backup Data**"), which Service Provider shall securely isolate and protect from any further Processing, except to the extent required by Applicable Laws. To the extent required by Applicable Laws, Service Provider will delete such Backup Data when the archived or backup system relating to such Backup Data is restored to an active system or is next accessed or used for further Processing or any commercial purpose. If required by law to retain Customer Personal Data, Service Provider will continue to ensure the confidentiality of such Customer Personal Data and only Process Customer Personal Data as necessary for the purpose specified in the Applicable Laws that require its storage.

12. Relevant Records and Audit Rights.

12.1. Upon Customer's request, Service Provider shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and/or Applicable Laws.

12.2. At Customer's expense (where permitted by Applicable Laws), Service Provider shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer ("**Mandated Auditor**") of any premises where the Processing of Customer Personal Data takes place in order to assess compliance with this DPA and/or Applicable Laws, and shall provide reasonable access to the Mandated Auditor to inspect, audit, and copy any relevant records, processes, and systems documents in order that Customer may satisfy itself that the provisions of this DPA are being complied with. Audits and inspections shall be conducted no more than once per year, during the term of the Agreement, and during regular business hours.

13. **International Data Transfers**. Customer agrees that Service Provider has authority to transfer any Customer Personal Data internationally or, in the case of Customer Personal Data received from Customer within the European Economic Area ("**EEA**") or United Kingdom ("**UK**"), outside the EEA or UK. Service Provider shall ensure that such transfer (and any onward transfer thereafter): (i) is pursuant to a written contract including adequate provisions relating to security and confidentiality of any Customer Personal Data; (ii) is made pursuant to a legally enforceable mechanism for such cross-border data transfers of Customer Personal Data under relevant laws; (iii) is made in compliance with this DPA; and (iv) otherwise complies with relevant privacy laws. With respect to facilitating international transfers of Customer Personal Data of EEA and UK residents, and by entering into the Agreement and DPA, Customer is deemed to have signed the EEA Standard Contractual Clauses approved by the European Commission in decision 2021/914 ("**SCCs**"), including the UK International Data Transfer Addendum to the EEA SCC's (the "**UK Addendum**") attached collectively hereto as Schedule 3 (or any other successor set of contractual clauses and addenda approved for use in the EEA and UK). In case of conflict, such attachments with SCCs or specific provisions shall take precedence where applicable over the terms of the Agreement.

14. **Indemnification**. In addition to any indemnification provisions in the Agreement, Customer will indemnify, defend and hold harmless Service Provider, its parents, subsidiaries, and Affiliates and all of their directors,

officers, agents and employees from and against any and all third-party claims, including without limitation claims or actions by applicable government agencies, arising out of or related to: (a) any actual or alleged breach by Customer of the Applicable Laws; (b) Customer's breach of the terms of this DPA; or (c) a claim by a Data Subject or other third party arising from an action or omission by Service Provider to the extent that such action or omission resulted from Customer's instructions. Service Provider may, at its option and expense, participate and appear on an equal footing with Customer in the defense of any claim related to this DPA that is conducted by Customer as set forth herein. Customer may not settle any claim regarding this DPA without Service Provider's prior written approval. Notwithstanding anything to the contrary set forth in the Agreement, any indemnification, defense or hold harmless obligations set forth herein are not subject to the limitation of liability provisions in the Agreement.

15. **General Terms** Pursuant to the Agreement, Service Provider reserves the right, in its sole discretion, to modify or replace any part of this DPA by posting the revised DPA on Service Provider's website and (announcing the change(s) to Service Provider's subscriber base, which may be done via generally distributed (including by electronic mail or within the Services) product release notes. Any such modifications shall take effect thirty (30) days (or less, if reasonably necessary) following the date of notice and in which case Beyond may require Customer to provide consent to the updated DPA in a specified manner before further use of the Services is permitted. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either: (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. Customer is responsible for any costs and expenses arising from Service Provider's compliance with Customer's instructions or requests pursuant to the Agreement (including this DPA) which fall outside the standard functionality made available generally through the Services. Customer and Service Provider expressly recognize and agree that this DPA includes provisions addressed in other portions of the Agreement. Customer and Service Provider hereby agree that the terms and conditions set out herein in this DPA shall be added as an addendum to the Agreement. This DPA and the other portions of the Agreement shall be read together and construed, to the extent possible, to be in concert with each other. In respect of any conflict between the Agreement and this DPA, the provisions which provide the greatest protection of the Customer Personal Data shall prevail; provided, however, that in no event shall this DPA be deemed to eliminate, limit, or otherwise diminish either party's obligations or commitments under portions of the Agreement.

SCHEDULE 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Schedule 1 includes details of the Processing of Customer Personal Data.

Categories of Data Subjects

- Prospective and current clients and customers of Customer (e.g. guests who would engage in a short term rental with Customer's listed properties) who are natural persons.

Categories of Customer Personal Data Transferred

- Personal contact details such as first and last name, email address, phone number, physical address, and booking reservation records
- IP address, user session activity
- Such other Customer Personal Data as may be submitted by Customer as reasonably necessary for Customer to receive or use the Services.

Nature of the Processing of Customer Personal Data

Service Provider will Process Customer Personal Data as necessary to perform the Services under the Agreement including collection, storage, organization, structuring, retrieval, modifying, erasing and as otherwise contemplated by the Services pursuant to the Agreement.

Purpose of the Processing of Customer Personal Data

The performance of the Services as described in the Agreement such as to provide Customer a revenue management platform.

SCHEDULE 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Service Provider shall adhere to the following technical and organizational measures.

Physical Access Control

All of Service Provider's offices require both building and office door authentication.

Logical Access Control

Systems access control is managed through LDAP and OAuth2 compatible Google Cloud Identity, when possible. MFA is enforced for all employees on Google Cloud Identity. All access and changes to server infrastructure is logged and tracked through Google Cloud audit logs. All server systems are protected by IPS Google Cloud Armor.

Data Access Control

Every Service Provider employee and contractor has access to all details listed in Schedule 1 subject to Service Provider's data warehousing program. This is necessary to properly provide customer support.

Data Transfer Control

All data transmissions between Service Provider and external third parties occur over RSA 2048 encrypted channels and all sync events are logged. All server data at rest is AES-256 encrypted.

Input Control

Personal data modification triggered through the application can be tracked back with application logs for up to 30 days.

Availability Control

Automatic database backups happen continuously in addition to real time replication of critical systems databases.

Data Separation

Data collected for different purposes is stored in physically separated databases.

Data protection by design and by default

Service Provider only collects Customer Personal Data as expressly needed for providing services to customers and providing needed support.

SCHEDULE 3: STANDARD CONTRACTUAL CLAUSES (EEA) AND UK ADDENDUM

1. The EEA SCCs are completed as follows:
    a. Module 2 (Controller to Processor) will apply.
    b. In Clause 7, the optional docking clause will not apply.
    c. In Clause 9, option 2 will apply, and the time period for prior notice of sub-processors is 10 days.
    d. In Clause 11, the optional clause will not apply.
    e. In Clause 13, Option 1 will apply if Customer has an establishment in the European Union; Option 2 will apply if Customer is not established in the European Union and has an appointed representative; and Option 3 will apply if Customer has neither an establishment nor a representative in the European Union.
    f. In Clause 17 (Option 1), the law of Spain will apply.
    g. In Clause 18(b), disputes will be resolved in the courts of Spain.
2. The EEA SCCs, Annex 1, Part A is completed as follows
    a. Data Exporter: Customer.
    b. Contact Details: Customer account address and email address.
    c. Data Exporter Role: Controller.
    d. Signature and Date: By entering into the Agreement, Customer is deemed to have signed these SCCs, including the UK Addendum.
    e. Activities relevant to the data transferred under the SCCs: utilizing the Services described in the Agreement provided by Service Provider.
    f. Data Importer: Ten Twenty Four, Inc. d/b/a Beyond Pricing.
    g. Contact Details: Beyond Pricing legal@beyondpricing.com.
    h. Data Importer Role: Processor.
    i. Signature & Date: By entering into the Agreement, Customer is deemed to have signed these SCCs, including the UK Addendum.
    j. Activities relevant to the data transferred under the SCCs: providing the Services described in the Agreement to Customer.
3. The EEA SCCs, Annex 1, Part B is completed as follows:
    a. Categories of data subjects whose personal data is transferred: See Schedule 1.
    b. Categories of personal data transferred: See Schedule 1.
    c. Sensitive data transferred: N/A.
    d. The frequency of transfer: Continuous.
    e. Nature of the processing: See Schedule 1.
    f. Purpose(s) of the data transfer and further processing: See Schedule 1.
    g. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: The term of the Agreement and pursuant to Section 11 of the DPA.
    h. For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: The subject matter, nature, and duration of Processing undertaken by subprocessors will be the same as set forth in this Annex 1.B with respect to Service Provider.
4. The EEA SCCs, Annex, Part C is completed as follows: The competent supervisory authority will be the supervisory authority that has supervision over the Data Exporter in accordance with Clause 13 of the SCCs.
5. The EEA SCCs, Annex II, is completed as follows: Schedule 2 serves as Annex II of the SCCs.
6. The UK Addendum is completed as follows:
    a. Part 1: Tables
        i. Table 1: Parties – The Parties as detailed in Section 2 to this Schedule 2.
        ii. Table 2: Selected SCCs, Modules and Selected Clauses – as detailed in Section 1 of this Schedule 2.
        iii. Table 3: Appendix Information – means the information which must be provided for the selected modules as set out in the Appendix of the SCCs (other than the Parties), and which is set out in Sections 2, 3, and 5 of this Schedule 2.
        iv. Table 4: Ending this Addendum when the Approved Addendum Changes – The Importer may end the UK Addendum as set out in Section 19 of the UK Addendum.
    b. Part 2
        i. Part 2: Mandatory Clauses – Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in

accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses.