base.

DATA PROCESSING ADDENDUM

Customer and Base (each a "Party" and collectively the "Parties") enter into this Data Processing Addendum (including the annexes attached hereto, this "DPA"), which forms part of the Base.com Terms of Use (as amended, the "Agreement") between the Parties and becomes effective upon Customer's acceptance of the Agreement.

1. Definitions

For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

(a) Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

(b) Applicable Data Protection Laws means the privacy, data protection and data security laws and regulations applicable to Base's Processing of Personal Data under the Agreement, including, as and to the extent applicable, the State Privacy Laws and GDPR.

(c) Controller means the entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, including, as applicable, any "business" or "controller" as such term is defined by the California Consumer Privacy Act (the "CCPA") or other State Privacy Laws.

(d) Customer Data means information provided or otherwise made available by or on behalf of Customer to Base for Processing on Customer's behalf to perform the Services.

(e) Data Subject means the identified or identifiable natural person to whom Personal Data relates.

(f) EEA means the European Economic Area.

(g) GDPR means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("UK GDPR"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "Articles" and "Chapters" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(h) Information Security Incident means a breach of Base's security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Base's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

(i) Personal Data means Customer Data that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Laws or information of a similar character regulated thereby, provided that Personal Data does not include such information pertaining to Customer's business contacts who are Customer personnel or such information that Base receives, collects, or generates independently of the Services and not from or on behalf of Customer.

(j) Process or Processing means any operation or set of operations which is performed by Base (or on Base's behalf) for Customer under the Agreement on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(k) Processor means the entity that Processes Personal Data on behalf of the Controller, including, as applicable, any "service provider" or "contractor" as those terms are defined by the CCPA.

(l) Restricted Transfer means the disclosure, grant of access or other transfer of Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "EU Restricted Transfer"); (ii) in the context of the UK, any country or territory outside the UK which does not benefit from an adequacy decision from the UK Government (a "UK Restricted Transfer"); and, in each case, which would be prohibited without a legal basis under applicable data protection law (including Chapter V of the GDPR, where applicable).

(m) SCCs means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(n) Security Measures has the meaning given in Section 4(a) (Base Security Measures).

(o) Services has the meaning given in the Terms.

(p) State Privacy Laws means, collectively, the comprehensive state-specific data privacy laws (and any implementing regulations) currently in effect and applicable to Base's Processing of Personal Data under the Agreement.

(q) Subprocessors means Base's Affiliates and third parties that Base engages to Process Personal Data in relation to the Services.

(r) Supervisory Authority means any entity with the authority to enforce Applicable Data Protection Laws, including: (i) in the context of the EEA and the EU GDPR, any entity falling within the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, the UK Information Commissioner's Office.

(s) UK Transfer Addendum means 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 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof.

2. **Duration and Scope of DPA**

(a) This DPA will remain in effect so long as Base Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

(b) Processing of Personal Data subject to the GDPR shall be subject to Annex 2 (European Annex).

(c) Processing of Personal Data subject to the State Privacy Laws with respect to which Customer is a Business, Controller, Processor, or Service Provider (as such terms are defined in State Privacy Laws) shall be subject to Annex 3 (State Privacy Laws Annex) to this DPA.

3. **Customer Instructions**

Base will Process Personal Data only in accordance with Customer's documented instructions to Base, including as set forth in this DPA, the Agreement, any applicable order form(s), and any other written instructions provided by Customer from time to time that are consistent with the Agreement and this DPA. To the extent Customer requests instructions that are outside the scope of the Services or that would require Base to materially change the Services or undertake additional work not contemplated by the Agreement, the Parties will agree to such instructions in a mutually executed amendment to this DPA or other written agreement. By entering into this DPA, Customer instructs Base to Process Personal Data to provide the Services and to perform its other obligations and exercise its rights under the Agreement. The Parties acknowledge and agree that the details of Base's Processing of Personal Data (including the respective roles of the Parties relating to such Processing) are as described in Annex 1 (Data Processing Details) to the DPA.

4. **Security**

(a) Base Security Measures. Base will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data as described in Annex 4 (the "Security Measures"), taking into account the state of the

art, the costs of implementation, and the nature, scope, context and purposes of Processing and the risks to Data Subjects. Base may update the Security Measures from time to time, including to maintain or improve security or address changes in Applicable Data Protection Laws, so long as the updated measures do not materially decrease the overall protection of Personal Data.

(b) Security Compliance by Base Staff. Base shall require that its personnel who are authorized to access Personal Data are subject to appropriate confidentiality obligations.

(c) Information Security Incidents. Base will notify Customer without undue delay, no later than 48 hours after detection, of any Information Security Incident of which Base becomes aware. Such notifications will describe, to the extent then known, available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Base recommends Customer take to address the Information Security Incident. Base's notification of or response to an Information Security Incident will not be construed as Base's acknowledgement of any fault or liability with respect to the Information Security Incident. Base shall reasonably cooperate with Customer and take such commercially reasonable steps, to the extent within Base's control, as may be reasonably requested by Customer and mutually agreed in good faith by the Parties to assist in the investigation of any such Information Security Incident. Customer is solely responsible for complying with notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Information Security Incident. If Customer determines that an Information Security Incident must be notified to any Supervisory Authority, any Data Subject(s), the public or others under Applicable Data Protection Laws, to the extent such notice directly or indirectly refers to or identifies Base, where permitted by applicable law, Customer agrees to (i) notify Base in advance, and (ii) in good faith, consult with Base and consider any clarifications or corrections Base may reasonably recommend or request to any such notification, which: (a) relate to Base's involvement in or relevance to such Information Security Incident; and (b) are consistent with applicable laws.

(d) Customer's Security Responsibilities and Assessment

(i) Customer's Security Responsibilities. Customer agrees that, without limitation of Base's obligations under Section 4 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Customer provides or makes available for Base to access in order to provide the Services; and (d) backing up Personal Data, as applicable.

(ii) Customer's Security Assessment. Customer acknowledges that it has evaluated the Services, the Security Measures and Base's commitments under this DPA and, based on information made available by Base, determines that they are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

5. **Data Subject Rights**

(a) Data Subject Request Assistance. Base will (taking into account the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary and technically feasible for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by Data Subjects to exercise their rights under Applicable Data Protection Laws ("Data Subject Requests") with respect to Personal Data in Base's possession or control. Customer shall compensate Base for any such assistance, to the extent such assistance requires work beyond the Services, at Base's then-current professional services rates, which shall be made available to Customer upon request, and Base will, upon request, provide Customer with a good-faith estimate of applicable fees.

(b) Customer's Responsibility for Requests. If Base receives a Data Subject Request, Base will (i) promptly notify Customer (unless prohibited by applicable law); and (ii) advise the Data Subject to submit the request to Customer. Customer will be solely responsible for responding to any such request, unless otherwise required by applicable law.

6. **Customer Responsibilities**

(a) Customer shall ensure (and is solely responsible for ensuring) that it has provided all notices to, and obtained all consents and permissions from, third parties (including, without limitation, Data Subjects), and has reserved all necessary rights, in each case, as may be required under Applicable Data Protection Laws for Base to Process Personal Data as contemplated by the Agreement.

(b) Customer represents and warrants to Base that Customer Data does not and will not contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords or other credentials for third-party online accounts (other than credentials created for and used solely to access the Services); credentials to any financial accounts; tax return data; any payment card information subject to the Payment Card Industry Data Security Standard; personal data of children under 16 years of age; or any other information that falls within any special categories of data (as defined in Applicable Data Protection Laws) ("**Restricted Data**"), in each case unless the Parties have otherwise agreed in writing prior to the submission of such data to the Services. For clarity, Restricted Data does not include the business or company registration or tax identification numbers (such as VAT or TIN numbers), or the order, invoice, billing, contact and delivery details, that the System is designed to Process in the ordinary course of providing the Services.

(c) Customer shall ensure that there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Base of Personal Data in accordance with this DPA and the Agreement (including any and all instructions issued by Customer from time to time in respect of such Processing) as required under all Applicable Data Protection Laws (including, where applicable, Articles 6, 9(2) and/or 10 of the GDPR).

(d) Customer shall ensure that all Data Subjects have (i) been presented with all required notices and statements (including as required by Articles 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Base of Personal Data.

7. **Subprocessors**

(a) Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Base's Affiliates as Subprocessors and generally authorizes Base to engage third parties as Subprocessors in accordance with this Section 7.

(b) Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available in Annex 5 of this DPA (the "Subprocessor List"). Base may continue to use those Subprocessors already engaged by Base as of the effective date of this DPA.

(c) Requirements for Subprocessor Engagement. When engaging any Subprocessor, Base will enter into a contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Base shall remain responsible for the performance of all obligations subcontracted to the Subprocessor and shall be liable for all acts and omissions of the Subprocessor to the same extent as Base would have been had it performed the Processing itself. Where the GDPR applies, Customer authorizes Base to grant authorizations and issue instructions to Subprocessors within the meaning of Article 29 of the GDPR, to the extent necessary to perform the Services and subject to this DPA.

(d) Opportunity to Object to Subprocessor Changes. When Base engages any new Subprocessor after the effective date of the DPA, Base will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the Subprocessor List and providing written notice (including by email) to Customer's designated contact for Services-related communications, or by other means permissible under the Agreement. If Customer objects to such engagement in a written notice to Base within ten (10) days after receipt of such notice on reasonable grounds relating to the protection of Personal Data, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written

notice to Base and pay Base for all amounts due and owing under the Agreement as of the date of such termination. If the Customer continues to use the Services after the expiry of the ten (10) day objection period, including by failing to delete its Account, the Customer shall be deemed to have withdrawn any objection and to have consented to the engagement of the new Subprocessor.

8. **Audits**

Reviews and Audits of Compliance. Customer may audit Base's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by Applicable Data Protection Laws solely to the extent Customer is legally required to conduct such additional audit or a competent Supervisory Authority with jurisdiction over Customer requires it, in each case upon Customer's written request providing reasonable detail and, where available, supporting documentation of the applicable requirement. Base will contribute to such audits by providing Customer with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Base may object to the auditor if the auditor is, in Base's reasonable opinion, not independent, a competitor of Base, or otherwise manifestly unsuitable. Such objection by Base will require Customer to appoint another auditor or conduct the audit itself. To request an audit, Customer must submit a proposed audit plan to Base at least two weeks in advance of the proposed audit date and any person participating in the audit on Customer's behalf, including any third-party auditor, must be subject to confidentiality obligations mutually acceptable to the Parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Base will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Base security, privacy, employment or other relevant policies). Base will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 8 shall require Base to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Base has confirmed there have been no known material changes in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Base's safety, security or other relevant policies, and may not unreasonably interfere with Base business activities. Any audit or inspection under this Section 8 is limited to the review of relevant documentation, records, policies and information and the receipt of written responses from Base, and does not extend to access to Base's live production systems, source code or premises, or to Personal Data or other data of Base's other customers. Customer will promptly notify Base of any non-compliance discovered during the course of an audit and provide Base any audit reports generated in connection with any audit under this Section 8, unless prohibited by Applicable Data Protection Laws. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. Any audits are at Customer's sole expense. Customer shall reimburse Base for any reasonable, documented costs (including reasonable internal time expended by Base and any third parties in connection with any audits or inspections under this Section 8 at Base's then-current professional services rates, which shall be made available to Customer upon request). Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

9. **Return and Deletion**

(a) Subject to Sections 9(b) and 9(c), upon the date of cessation of any Services involving the Processing of Personal Data (the "Cessation Date"), Base shall promptly cease all Processing of Personal Data for any purpose other than for storage and Processing necessary to effect the return, deletion, or anonymization of such Personal Data, or as otherwise permitted or required under this DPA or applicable law.

(b) Subject to Section 9(d), to the extent technically feasible in the circumstances (as determined in Base's sole discretion), on written request to Base (to be made within seven (7) days after the Cessation Date ("Post-cessation Storage Period")), Base shall within a commercially reasonable period following receipt of such request, as elected by Customer in such request, either (i) return a complete copy of all Personal Data within Base's possession to

Customer by secure file transfer or other commercially reasonable secure method, promptly following which Base shall delete or anonymize all other copies of such Personal Data, or (ii) delete or anonymize all Personal Data within Base's possession.

(c) In the event that during the Post-cessation Storage Period, Customer does not instruct Base in writing to either delete or return Personal Data pursuant to Section 9(b), Base shall, within a commercially reasonable time after the expiry of the Post-cessation Storage Period, either (at its option) delete or render anonymous all Personal Data then within Base's possession, custody or control to the fullest extent technically feasible in the circumstances.

(d) Base may retain Personal Data to the extent permitted or required by applicable law, for no longer than such applicable law requires, provided that Base shall (i) maintain the confidentiality of all such Personal Data and protect it in accordance with the Security Measures, (ii) Process such Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention, and (iii) delete or anonymize such Personal Data once it is no longer permitted or required to be retained under applicable law.

(e) Base may further retain Personal Data contained in automated backup or archival copies generated in the ordinary course of Base's operations, provided that such copies (i) remain subject to the Security Measures, (ii) are not restored to production or otherwise accessed or Processed for any purpose other than disaster recovery or business continuity, and (iii) are deleted or overwritten in accordance with Base's standard backup retention cycle.

10. **Artificial Intelligence and Automated Processing**

(a) Base shall not use Personal Data to train, fine-tune, develop, or improve any artificial intelligence or machine learning model, whether Base's own or a third party's, unless (a) such use is reasonably necessary to provide the Services in accordance with the Customer's documented instructions, or (b) expressly authorized by the Customer.

(b) Base shall prohibit its Subprocessors, including any AI model providers, from using Personal Data for their own model training, fine-tuning, development, or improvement purposes, unless (a) such use is reasonably necessary to provide the Services in accordance with the Customer's documented instructions to Base, or (b) expressly authorized by the Customer.

(c) If the Services involve automated decision-making that produces legal or similarly significant effects on Data Subjects, Base shall: (a) disclose the existence of such processing to the Customer; (b) to the extent reasonably available to Base, provide meaningful information about the logic involved without requiring disclosure of Base's trade secrets or confidential information; and (c) reasonably cooperate with the Customer, as required by Applicable Data Protection Laws, to enable Data Subjects to exercise applicable rights under such laws relating to automated decision-making.

(d) Nothing in this DPA restricts Base from collecting, generating and using aggregated, anonymized, de-identified or statistical data derived from the Processing, provided that such data does not identify, and cannot reasonably be used to identify, Customer or any Data Subject. Such data does not constitute Personal Data or Customer Data and is not subject to the return and deletion obligations in Section 9.

11. **Miscellaneous**

(a) Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the Parties acknowledge and agree that Base's access to Personal Data does not constitute part of the consideration exchanged by the Parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Base to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement; (b) to Customer's contact details for data protection set out in Annex 1; (c) to Base's primary points of contact with Customer; or (d) to any email address designated by Customer in writing for the purpose of receiving Services-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

(b) Base agrees to cooperate in good faith with Customer to consider any amendments that may be reasonably necessary to address compliance with the Applicable Data Protection Laws.

(c) Base may, on written notice, vary this DPA solely to the extent necessary to maintain compliance with Applicable Data Protection Laws from time to time, provided that any such variation shall not materially reduce the protections afforded to Personal Data or materially increase Customer's obligations under this DPA without Customer's written agreement, and may include varying or replacing the SCCs in accordance with Paragraph 3.3 (Adoption of new transfer mechanism) of Annex 2 (European Annex).

(d) To the extent permitted by Applicable Data Protection Laws and the SCCs (if and as they apply), the total aggregate liability of either Party to the other Party, however arising, under or in connection with this DPA and the SCCs (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the Agreement; provided that nothing in this Section 11(d) will affect any person's liability to Data Subjects under the third-party beneficiary provisions of the SCCs (if and as they apply).

(e) Base shall not be liable to the Customer for any administrative fine, penalty or other administrative sanction imposed on Customer by a Supervisory Authority or other competent authority in connection with the Processing, irrespective of cause.

(f) In the event of any conflict or inconsistency between (i) this DPA and the Agreement, this DPA shall prevail, or (ii) any SCCs entered into pursuant to Paragraph 3 of Annex 2 (European Annex) and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

Annex 1
Data Processing Details

BASE / 'DATA IMPORTER' DETAILS

Contact Details for Data Protection: Data Protection Officer / privacy@base.com

Base Activities: Software-as-a-Service platform (base.com) enabling business Customers to manage and automate online sales across multiple sales channels, including order, product, inventory, shipping, invoicing and messaging management and related third-party integrations; implementation services; other services agreed between the Parties.

Role: Processor (or Subprocessor, as applicable)

CUSTOMER / 'DATA EXPORTER' DETAILS

Customer Activities: Customer's activities relevant to this DPA are the use and receipt of the Services under and in accordance with, and for the purposes anticipated and permitted in, the Agreement as part of its ongoing business operations.

Role: Controller or Processor (as applicable)

Categories of Data Subjects: Relevant Data Subjects include any Data Subjects whose Personal Data Customer causes Base to Process in connection with the Services, including End-users and other users of Customer's products and services, and Customer's personnel (including employees and contractors) and other business contacts or representatives of Customer.

Categories of Personal Data: Relevant Personal Data includes any categories of Personal Data Customer causes Base to Process as part of the provision of the Services, including:

- **Personal details –** for example any information that identifies the Data Subject, including name and contact information.
- **Authentication details –** for example usernames, passwords or PIN codes used to access the Services, security questions, authentication tokens, and other access protocols.
- **Technological details –** for example internet protocol (IP) addresses, unique identifiers and numbers (including unique identifiers in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.
- **Commercial and transactional details –** for example company or business name, honorific or title (e.g., Mr/Ms), business or company registration and tax identification numbers (such as VAT or TIN numbers), billing and delivery addresses, email addresses and telephone numbers, and order, invoice and transaction details.

Sensitive Categories of Data, and associated additional restrictions/safeguards:

Categories of sensitive data, and additional safeguards: None – as noted in Section 6(b) of the DPA, Customer agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the SCCs), must not be submitted to the Services without the Parties' prior written agreement.

Frequency of transfer: Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.

Nature of the Processing: Processing operations required in order to provide the Services and perform Base's obligations in accordance with the Agreement and this DPA.

Purpose of the Processing: As necessary to provide the Services as initiated by Customer in its use thereof, and to comply with Customer's documented instructions as permitted under and in accordance with the terms of this DPA and the Agreement.

Duration of Processing / Retention Period: For the period determined in accordance with the Agreement and DPA.

Transfers to (sub)processors: Transfers to Subprocessors are as, and for the purposes, described from time to time in the Subprocessor List (Annex 5).

base.

Annex 2

European Annex

1. PROCESSING OF PERSONAL DATA

1.1. Where Base receives an instruction from Customer that, in its reasonable opinion, infringes the GDPR, Base shall inform Customer.

1.2. Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing of Personal Data by or on behalf of Base pursuant to or in connection with the Agreement shall be in strict compliance with the GDPR and all other applicable laws.

2. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

2.1. Base, taking into account the nature of the Processing and the information available to Base, shall provide reasonable assistance to Customer, at Customer's cost, upon Customer's written request, to the extent reasonably necessary and technically feasible, with any data protection impact assessments and prior consultations with Supervisory Authorities as may be required of Customer under Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Personal Data by Base.

2.2. Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Base (at Base's then-current professional services rates) in Base's provision of any cooperation and assistance provided to Customer under Paragraph 2.1, and shall on demand reimburse Base for any such costs incurred by Base.

3. RESTRICTED TRANSFERS

EU Restricted Transfers

3.1. To the extent that any Processing of Personal Data under this DPA involves an EU Restricted Transfer from Customer to Base, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be:

(a) populated in accordance with Part 1 of Attachment 1 to Annex 2 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

UK Restricted Transfers

3.2. To the extent that any Processing of Personal Data under this DPA involves a UK Restricted Transfer from Customer to Base, the Parties shall comply with their respective obligations set out in the SCCs (as varied by the UK Transfer Addendum), which are hereby deemed to be:

(a) varied to address the requirements of the UK GDPR in accordance with the UK Transfer Addendum and populated in accordance with Part 2 of Attachment 1 to Annex 2 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

Adoption of new transfer mechanism

3.3. Base may, on notice, vary this DPA and replace the relevant SCCs with:

(a) any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly to the extent necessary to maintain compliance with Applicable Data Protection Laws, provided that any such replacement does not materially decrease the overall protection of Personal Data under the SCCs (e.g., standard data protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the GDPR); or

(b) another valid transfer mechanism, other than the SCCs, that Base reasonably determines is necessary to maintain compliance with Chapter V of the GDPR for the relevant transfer(s) and that does not materially diminish the data protection safeguards for Personal Data under this DPA.

Provision of full-form SCCs

3.4. In respect of any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject or further Controller (where applicable) – on specific written request (made to the contact details set out in Annex 1 (Data Processing Details); accompanied by suitable supporting evidence of the relevant request), and to the extent required to evidence Customer's compliance with Applicable Data Protection Laws, Base shall provide Customer within a reasonable time with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with Attachment 1 to Annex 2 (European Annex) in respect of the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage.

Operational clarifications

3.5. When complying with its transparency obligations under Clause 8.3 of the SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, Base's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

3.6. Where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Base to notify any third-party controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer.

3.7. For the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

3.8. The terms and conditions of Section 7 of the DPA apply in relation to Base's appointment and use of Subprocessors under the SCCs. Any approval by Customer of Base's appointment of a Subprocessor that is given expressly or deemed given pursuant to that Section 7 constitutes Customer's documented instructions to effect disclosures and onward transfers of Personal Data to such Subprocessor solely in connection with the Services, if and as required under Clause 8.8 of the SCCs.

3.9. The audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in Section 8 of the DPA.

3.10. Certification of deletion of Personal Data as described in Clauses 8.5 and 16(d) of the SCCs shall be provided only upon Customer's written request.

Attachment 1

To Annex 2 (European Annex)

POPULATION OF SCCs

Note

- In the context of any EU Restricted Transfer, the SCCs populated in accordance with Part 1 of this Attachment 1 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 3.1 of Annex 2 (European Annex) to the DPA).
- In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and populated in accordance with Part 2 of this Attachment 1 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 3.2 of Annex 2 (European Annex) to the DPA).

PART 1: POPULATION OF THE SCCs

1. SIGNATURE OF THE SCCs:

Where the SCCs apply in accordance with Paragraph 3.1 of Annex 2 (European Annex) to the DPA, each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. MODULES

The following modules of the SCCs apply in the manner set out below (having regard to the role(s) of Customer under the Agreement and as set out in Annex 1 (Data Processing Details) to the DPA):

(a) Module Two of the SCCs applies to any EU Restricted Transfer involving Processing of Personal Data in respect of which Customer is a Controller in its own right; and/or

(b) Module Three of the SCCs applies to any EU Restricted Transfer, UK Restricted Transfer involving Processing of Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person.

3. POPULATION OF THE BODY OF THE SCCs

3.1. For each Module of the SCCs, the following applies as and where applicable to that Module and the Clauses thereof:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 9:

(i) OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Subprocessors shall be the notice period set out in Section 7(d) of the DPA (currently ten (10) days); and

(ii) OPTION 1: SPECIFIC PRIOR AUTHORISATION is not used and that optional language is deleted; as is, therefore, Annex III to the Appendix to the SCCs.

(c) In Clause 11, the optional language is not used and is deleted.

(d) In Clause 13, all square brackets are removed, and all text therein is retained.

(e) In Clause 17:

i. OPTION 1 applies, and the Parties agree that the SCCs shall be governed by the law of Poland in relation to any EU Restricted Transfer; and

ii. OPTION 2 is not used and that optional language is deleted.

(f) For the purposes of Clause 18, the Parties agree that any dispute arising from the SCCs in relation to any EU Restricted Transfer shall be resolved by the courts of Poland, and Clause 18(b) is populated accordingly.

3.2. In this Paragraph 3, references to “Clauses” are references to the Clauses of the SCCs.

4. POPULATION OF ANNEXES TO THE APPENDIX TO THE SCCs

4.1. Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Annex 1 (Data Processing Details) to the DPA, with:

(a) Customer being ‘data exporter’; and

(b) Base being ‘data importer’.

4.2. Part C of Annex I to the Appendix to the SCCs is populated as below:

The competent supervisory authority shall be determined as follows:

- Where Customer is established in an EU Member State: the competent supervisory authority shall be the supervisory authority of that EU Member State in which Customer is established.
- Where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which Customer’s EU representative relevant to the processing hereunder is based (from time-to-time).
- Where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies, but Customer has not appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to Base’s contact point for data protection identified in Annex 1 (Data Processing Details) to the DPA, which must be an EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located.

4.3. Annex II to the Appendix to the SCCs is populated as below:

General:

- Please refer to Section 4 of the DPA and Annex 4 (Security Measures) to the DPA.
- In the event that Customer receives a Data Subject Request under the EU GDPR and requires assistance from Base, Customer should email Base’s contact point for data protection identified in Annex 1 (Data Processing Details) to the DPA.

Subprocessors: When Base engages a Subprocessor under these Clauses, Base shall enter into a binding contractual arrangement with such Subprocessor that, to the extent applicable to the nature of the services provided by such Subprocessor, imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the DPA – including in respect of:

- appropriate technical and organizational information security measures;
- notification of Information Security Incidents to Base;
- return or deletion of Personal Data, as and where required; and the engagement of further Subprocessors.

PART 2: UK RESTRICTED TRANSFERS

1. UK TRANSFER ADDENDUM

1.1. Where relevant in accordance with Paragraph 3.2 of Annex 2 (European Annex) to the DPA, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below –

(a) Part 1 to the UK Transfer Addendum. As permitted by Section 17 of the UK Transfer Addendum, the Parties agree:

(i) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Data Processing Details) and the foregoing provisions of this Attachment 1 (subject to the variations effected by the Mandatory Clauses described in (b) below); and

(ii) Table 4 to the UK Transfer Addendum is completed by the box labeled 'Data Importer' being deemed to have been ticked.

(b) Part 2 to the UK Transfer Addendum. The Parties agree to be bound by the Mandatory Clauses of the UK Transfer Addendum.

1.2. In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in Paragraph 1.1 of this Part 2.

base.

Annex 3

State Privacy Laws Annex

1. For purposes of this Annex 3, the terms “business,” “controller,” “processor,” “commercial purpose,” “sell,” “share,” “service provider” and “contractor” shall have the respective meanings given thereto in the applicable State Privacy Laws, and “personal information” shall mean Personal Data to the extent it constitutes “personal information” or “personal data” (or a similar term) governed by the State Privacy Laws.

2. It is the Parties’ intent that with respect to any personal information, Base is a service provider, contractor and/or processor, as applicable under the State Privacy Laws. Base (a) acknowledges that personal information is disclosed by Customer only for limited and specified purposes described in the Agreement; (b) shall comply with applicable obligations under the State Privacy Laws and shall provide the same level of privacy protection to personal information as is required by the State Privacy Laws; (c) agrees that Customer has the right to take reasonable and appropriate steps to help to ensure that Base’s Processing of personal information is consistent with Customer’s obligations under the State Privacy Laws; (d) shall notify Customer in writing of any determination made by Base that it can no longer meet its obligations under the State Privacy Laws; and (e) agrees that Customer has the right, upon reasonable notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

3. Base shall not (a) sell or share any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Services, or as otherwise permitted by the State Privacy Laws; (c) retain, use or disclose the personal information outside of the direct business relationship between Base and Customer; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) collected from Base’s own interaction with any Data Subject to whom such personal information pertains, except as and to the extent permitted by the State Privacy Laws and necessary as part of Base’s provision of the Services. Base hereby certifies that it understands its obligations under this Section 3 and will comply with them.

4. Giving Customer notice of Subprocessor engagements in accordance with Section 7 of the DPA shall satisfy Base’s obligation under the State Privacy Laws to give notice of and an opportunity to object to such engagements.

5. Customer may conduct audits, in accordance with Section 8 of the DPA, to help ensure that Base’s use of personal information is consistent with Base’s obligations under the State Privacy Laws.

6. The Parties acknowledge that Base’s retention, use and disclosure of personal information authorized by Customer’s instructions documented in the Agreement and this DPA are integral to Base’s provision of the Services and the business relationship between the Parties.

Annex 4
Security Measures

GDPR implementation status

The GDPR implementation project has been completed, Base has and maintains the documents required by the GDPR, including a register of all categories of processing activities.

The personal data protection system is continually maintained and regularly reviewed. Independent audits of the personal data protection system are carried out once a year, and *ad hoc* audits are also carried out if necessary.

The level of security corresponds to the identified risks and is being continually improved. Base ensures a level of security of the entrusted data adequate to the risk of violating the rights and freedoms of natural persons, and in particular means of protecting the entrusted personal data against accidental destruction, loss, modification, and unauthorized disclosure.

Up-to-date risk analysis results are maintained for resources processing the entrusted personal data. A risk management plan is being implemented to maintain and continually improve the level of personal data security. If a vulnerability that may cause a significant risk is identified, it is taken into account as part of the risk management plan and assigned the appropriate priority.

Base has adopted data protection documentation covering all aspects of GDPR compliance. The organization's policies and procedures are regularly consulted, explained and, if necessary, updated in cooperation with the data protection officer's team.

Due to the full implementation of the ISO/IEC 27001 standard, the organization also has comprehensive documentation of the information security management system, which also includes the personal data protection system.

Personal data protection policies and procedures

Base has prepared and adopted policies and procedures for the protection of personal data in accordance with Article 24(2) of the GDPR and the requirements of the Polish supervisory authorities.

The policies and procedures for the protection of personal data have been communicated to Base's staff.

Base has prepared and implemented a security policy or instruction for managing ICT resources.

Base has prepared a procedure for the immediate reporting of security breaches to Customer.

Persons performing operations on personal data have been duly authorized to process personal data pursuant to Article 29 of the GDPR.

Base keeps a record of all categories of processing activities, which includes all information required under Article 30(2) of the GDPR.

Base is able to demonstrate compliance with the principles of personal data processing.

Employee awareness

Base ensures that before allowing the processing of personal data, the employed staff member will be familiarized with the applicable data protection policies and procedures.

Base ensures to improve the knowledge of its staff members through periodic training and other activities aimed at raising awareness in the field of personal data protection and information security.

Employees and associates of Base who participate in the processing of personal data are obliged to keep them secret.

Members of Base's staff who participate in the processing of entrusted personal data have received appropriate authorizations to process personal data, and their access to data and authorizations is limited in accordance with the need-to-know principle.

Management of violations, requests from natural persons, support for Customer in demonstrating compliance with the GDPR

Base has implemented a procedure in the event of detecting a possible data protection breach.

Base has the means to exercise the rights of data subjects, in particular, the right to limit processing and the right to be forgotten.

Base notifies Customer promptly of a breach of personal data protection - within the deadline specified in the provisions of the Addendum. Base responds to Customer's questions to the extent and within the deadlines necessary to fulfill the related obligations arising from the GDPR.

Data protection officer and other functions related to data protection

Base has appointed a Data Protection Officer whose status reflects the requirements of Article 38 of the GDPR and who performs all the tasks indicated in Article 39 of the GDPR.

Contact to the data protection officer: privacy@base.com.

The data protection officer is independent, and the decisions regarding the purposes and methods of processing rest with the representative of senior management and the owners of processes and resources.

In connection with the operation of the information security management system, persons performing functions meeting the requirements of the ISO/IEC 27001 standard have been appointed, in particular the Chief Information Security Officer.

Codes of conduct and certification mechanisms, information security

Base has implemented a full information security management system in accordance with the ISO/IEC 27001 standard and has a current certificate confirming the correct implementation and maintenance of the information security management system (ISMS), in accordance with the above-mentioned standard.

Audit and risk analysis

Base subjects its personal data protection system to regular, independent audits and security tests.

Base regularly identifies and classifies resources processing personal data, including in terms of existing and planned security measures, identified vulnerabilities, probability of occurrence, and severity of threats.

The level of information security is additionally monitored through the use of key performance indicators (KPIs).

Subcontractors

Base uses only the services of such third parties/subcontractors who have been previously verified in terms of ensuring an adequate level of protection of personal data.

Base verifies the adequacy of the guarantees provided by further processors, including, where appropriate, by asking to complete questionnaires and provide answers.

Data processing locations and data transfers, cloud computing

As a rule, Base processes personal data in data centers provided by specialized further processing entities indicated in the Terms, with the main supplier of the ICT infrastructure being Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg. Security guarantees from this entity are described at: https://aws.amazon.com/security/

All entrusted personal data are stored only within the infrastructure provided by specialized further processing entities. However, in order to process data on its own resources, Base has implemented physical security rules and rules regarding remote work security.

To the extent that the entrusted data is processed in the AWS cloud, Base evaluates the security measures used by the supplier and supplements them by using tools and configuration solutions selected by the Chief Information Security Officer and owners of resources. In particular, it uses data encryption, verification of the correctness of configuration solutions, usage monitoring, vulnerability scanning, network traffic filtering, event logging, access management, separation, segmentation and redundancy and load balancing solutions.

Physical security

The physical locations of personal data processing are covered by access control measures, including, where appropriate, an access card system, video monitoring, security agencies, and burglar alarms.

Resources involved in data processing by Base are physically separated from other organizations.

Security measures have been implemented to minimize the risk of losses resulting from physical and environmental threats, including, where appropriate, relevant threat detection systems, including fire protection systems.

Access rights to the area of personal data processing are regularly checked and, if necessary, withdrawn.

The process of safe data deletion and safe decommissioning of data media has been regulated.

Documents in paper form are protected against unauthorized access in accordance with the clean desk principle, and after established processing periods - destroyed using a shredder of a standard not lower than that corresponding to confidential documents.

Access control to IT systems

Authorizations within the IT systems are granted in accordance with the need-to-know principle; a password policy has been implemented.

Staff members are required to apply the principle of a clean desk and screen.

Access control measures such as encryption, two-step authentication, and VPN are used where appropriate.

Technical security, maintenance, and testing of equipment

The IT system used to process personal data is protected against power failures.

Hardware and software maintenance complies with the supplier’s recommendations.

A procedure for removing and destroying resources withdrawn from use has been adopted and applied.

The security of the server room corresponds to the current security standards.

Base ensures regular testing, measurement and assessment of the effectiveness of technical and organizational measures to ensure processing security.

Business continuity

Base has a business continuity plan.

Appropriate mechanisms for monitoring and detecting events that may affect information security and business continuity have been implemented.

Base is able to efficiently restore the availability of and access to personal data in the event of a physical or technical incident.

Base has implemented a backup policy covering the adequate scope, frequency, and testing.

Base has implemented disaster recovery and testing procedures.

Measures have been implemented to prevent unauthorized copies of data from the IT system and to secure backup copies.

Other GDPR requirements

Base implements new solutions according to the *privacy by design* principle.

Base processes the data according to the *privacy by default* principle.

Base keeps an inventory of the resources used in the processing of personal data.

Annex 5
List of Subprocessors

Customer approves Base's engagement of the following Subprocessors to provide services pursuant to the Agreement:

Sub-Processor	Registered Office / Place of Processing	Data Processing Activity
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg, Grand Duchy of Luxembourg / Place of processing: European Economic Area	Provision of cloud hosting and computing infrastructure on which the Services operate; processes Buyers' personal data stored and transmitted within that infrastructure.
OVH sp. z o.o.	ul. Swobodna 1, 50-088 Wrocław, Poland / Place of processing: Poland (European Economic Area)	Provision of server and cloud hosting infrastructure for the Services; processes buyers' personal data stored on that infrastructure.
Cloudflare, Inc.	101 Townsend Street, San Francisco, CA 94107, United States of America / Place of processing: European Economic Area and United States of America (transfers based on the EU Standard Contractual Clauses)	Content delivery network, DNS, traffic routing and security/anti-DDoS services, including delivery of the order page; processes buyers' personal data transmitted through those services.
Twilio Ireland Limited	3 Dublin Landings, North Wall Quay, Dublin 1, D01 C4E0, Ireland / Place of processing: European Economic Area	Sending SMS notifications to Buyers, where the merchant uses that functionality; processes buyers' telephone numbers and message content.
EmailLabs – Vercom S.A.	ul. Wierzbięcice 1B, 61-569 Poznań, Poland (KRS 0000535618) / Place of processing: Poland (European Economic Area)	Sending e-mail messages to Buyers, including messages generated from the order page; processes buyers' e-mail addresses and message content.
SendGrid – Twilio Inc.	101 Spear Street, Suite 500, San Francisco, CA 94105, United States of America / Place of processing: United States of America (transfers based on the EU Standard Contractual Clauses)	Fallback e-mail delivery provider for EmailLabs when sending messages to buyers; processes buyers' e-mail addresses and message content.
SMSAPI – LINK Mobility Poland sp. z o.o.	ul. Toszecka 101, 44-117 Gliwice, Poland (KRS 0000350201) / Place of processing: Poland (European Economic Area)	Sending SMS messages to Buyers; processes Buyers' telephone numbers and message content.

PrintNode Limited	2 Manor Farm Court, Old Wolverton Road, Old Wolverton, Milton Keynes MK12 5NN, United Kingdom (company no. 10383892) / Place of processing: United Kingdom (adequacy decision)	Printing of shipping labels; receives the recipient's data (name, address, contact details) contained on the label.
Affiliates of Base	As applicable	Supporting Base's performance of the Services