Omnistrate
Data Processing Addendum

Last Updated: September 15th, 2026

This Data Processing Addendum ("DPA") is incorporated into and forms part of the Master Services Agreement or other applicable written or electronic or subscription agreement or Platform Terms of Use ("**Agreement**") between the Omnistrate entity which entered into the Agreement ("**Omnistrate**") and the **Customer** signatory thereto. The parties agree that this DPA shall replace any existing DPA, or other data protection provisions the parties may have previously entered into in connection with the Services. In consideration of the mutual obligations set forth herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. The following obligations shall only apply to the extent required by Data Protection Laws with regard to the relevant Customer Personal Data, if applicable. The Parties agree and acknowledge that to the extent any personal data that originates from the United Kingdom (UK) and is subject to applicable UK data protection laws is being transferred by Customer to Omnistarte, the UK SCC Addendum shall apply.

Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions

(a) "**Agreement**" means the written or electronic agreement between Customer and Omnistrate for the provision of the Services to Customer.

(b) "**CCPA**" means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended by the California Privacy Rights Act of 2020 ("**CPRA**") or otherwise or superseded from time to time.

(c) "**Customer Personal Data**" means any Personal Data that is uploaded into the Cloud Services for storage or hosting and/or accessed by Omnistrate while processing on behalf of Customer in the course of providing Services.

(d) "**Data Protection Laws**" means all state, foreign laws and regulations related to data protection, security and privacy laws applicable to the processing of Customer Personal Data under the Agreement.

(e) "**EEA**" means the European Economic Area.

(f) **"EU GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(g) "**GDPR**" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

(h) "**Security Incident**" means an unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

(i) **"Sell" or "Sale"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means, Customer Personal Data to a third party for monetary or valuable consideration.

(j) "**Sub-processor**" means any Processor engaged by Omnistrate or its Affiliates to process Customer Personal Data. Sub processors may include third parties or Omnistrate's Affiliates.

(k) **"UK GDPR"** means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

(l) The terms "**Business**", "**collect**", "**Consumer**", "**Controller**", "**Data Subject**", "**Processor**," "**process**,", "**processing**" and "**Personal Data**", and "**Service Provider**" have the meanings given to them in applicable Data Protection Laws.

2. Scope of this DPA

This DPA applies where and only to the extent that Omnistrate processes Customer Personal Data on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement.

3. Roles and Scope of Processing

3.1 Role of the Parties. The parties acknowledge and agree that as between the parties, with regard to the Processing of Customer Personal Data under the Agreement, Customer may act as Controller and/or Processor of Customer Personal Data and Omnistrate may act as Processor and/or sub-processor of Customer Personal Data.

3.2 Customer as Controller of Customer Personal Data. If Customer is Controller of Customer Personal Data, Customer agrees that (i) it will comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Customer Personal Data and any processing instructions it issues to Omnistrate; and (ii) it has provided adequate notice and obtained (or will obtain) all appropriate and valid consents to disclose such Customer Personal Data to Omnistrate and rights necessary for Omnistrate to process Customer Personal Data pursuant to the Agreement and this DPA. The Customer shall notify Omnistrate of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Customer Personal Data that would impact Omnistrate's ability to comply with the Agreement, this DPA, or Data Protection Laws.

3.3 Customer as Processor of Customer Personal Data. If Customer is Processor of Customer Personal Data, Customer warrants on an ongoing basis that the relevant Controller has authorized: (i) Omnistrate's processing of Customer Personal Data as outlined in this DPA and in Exhibit A; (ii) Customer's appointment of Omnistrate as another processor; and (iii) Omnistrate's engagement of Sub-processors as described in Section 5 below.

3.4 Customer Instructions. Omnistrate will process Customer Personal Data only (i) for the purpose of providing the Services and in accordance with Customer's documented lawful instructions as set forth in the Agreement, unless otherwise required by applicable law, in which case Omnistrate will inform Customer of such Processing unless notification is prohibited by applicable law and this DPA; .(ii) as part of the direct business relationship between Customer and Omnistrate; or (iii) as permitted by law. Customer hereby instructs Omnistrate to Process Customer Personal Data: (a) to provide the Services to Customer; (b) to perform its obligations and exercise its rights under the Agreement and this DPA; and (c) as necessary to prevent or address technical problems with the Service. Omnistrate shall inform Customer if, in its opinion, Customer's processing instruction infringes applicable Data Protection Laws. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in this DPA. Omnistrate certifies that it understands the restrictions in this Section 3.4 and will comply with such restrictions.

3.5 Details of Data Processing

(a) Subject matter. The subject matter of the data processing under this DPA is Customer Personal Data.

(b) Duration of the processing. As between Omnistrate and Customer, the duration of the data processing under this DPA is the term of the Agreement.

(c) Purpose of the processing. Performance of the Services.

(d) Nature of the processing: Omnistrate will use and otherwise process Customer Personal Data only in accordance with Customer's documented instructions and as described and subject to the terms of the Agreement and this DPA.

(e) Categories of data subjects: The data subjects of Customer may include Customer's customers, employees, contractors, suppliers, and other third parties.

(f) Types of Customer Personal Data. Personal data processed under this DPA include Customer Personal Data. Customer acknowledges that it solely chooses the nature and types of Customer Personal Data and that Omnistrate will be generally unaware of the details of Customer Personal Data processed within the Services.

4. Data Transfers

4.1 Data Storage and Processing Facilities. Customer Personal Data will be stored in the United States. As part of providing the Services, including Support Services, Omnistrate, its Affiliates, or its Sub processors may access Customer Personal Data from locations outside the United States, except in territories subject to OFAC sanctions. Omnistrate ensures that such access is limited to what is necessary for the provision of Services and Support, and it will at all times implement appropriate safeguards to provide an adequate level of protection for Customer Personal Data, in compliance with applicable Data Protection Laws.

4.2 Cross-Border Transfers. For transfers of Customer Personal Data from the EEA, Switzerland, or the United Kingdom, Omnistrate will rely on an adequacy decision under Article 45 GDPR (or equivalent under UK law) where the transfer is to a country or territory recognized as providing

an adequate level of protection. Where no adequacy decision applies, Omnistrate will ensure compliance with GDPR Chapter V using Standard Contractual Clauses (SCCs) approved by the European Commission (Decision 2021/914/EU) for international transfers and/or supplementary safeguards such as encryption, access controls, and continuous monitoring to address any associated risks. The provisions outlined in Exhibit A form an integral part of this DPA and detail Omnistrate's commitments to safeguard Customer Personal Data during such transfers.

5. Sub processing

5.1 5.1 Authorized Sub processors. Customer agrees that in order to provide the Services, Omnistrate may engage Sub processors to process Customer Personal Data. A list of Omnistrate's authorized Sub processors is provided in Exhibit C of this DPA.

5.2 Sub processor Obligations. Where Omnistrate authorizes any Sub processor as described in Section 5.1 above:

1. Access to Customer Personal Data will be limited only to what is necessary to assist Omnistrate in providing or maintaining the Services, and Sub processor will be prohibited from accessing Customer Personal Data for any other purpose;

2. Omnistrate will enter or has already entered into a written agreement with the Sub processor imposing data protection terms that require the Sub processor to protect the Customer Personal Data to the standard required by applicable Data Protection Laws; and

3. Omnistrate will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub processor that cause Omnistrate to breach any of its obligations under this DPA.

Upon request and subject to any pre-existing confidentiality obligations, Omnistrate will provide Customer with all the relevant information it reasonably can in connection with its applicable Sub processor agreements when required to satisfy Customer’s obligations under applicable Data Protection Laws.

5.3 Sub processor Updates. Omnistrate will provide Customers with a 30-day prior notice via email if it intends to make any changes to its existing authorised list of Sub processors (Exhibit C). Customers may, within 15 days of notification, object in writing to the Omnistrate's appointment of a new Sub processor, provided that such objection is based on reasonable grounds relating to the processing of Customer Personal Data by the new Sub processor. In such an event, the parties will discuss such objections in good faith with a view to achieving resolution. If this is not possible, Customer has the right to suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

6. Security Measures and Security Incident Response

6.1 Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Omnistrate has implemented and will maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the

Customer Personal Data ("Security Measures"). Omnistrate's Security Measures align with industry standards and have been independently validated through SOC 2 Type II certification, ensuring compliance with stringent security, availability, and confidentiality requirements. Omnistrate continuously monitors and improves its security controls to safeguard Customer Personal Data in accordance with applicable Data Protection Laws and best practices.

6.2 Updates to Security Measures. Based on Omnistrate's security certifications and related information made available by Omnistrate, Customer has independently determined that the Services meet Customer's requirements and obligations under applicable Data Protection Laws. Customer acknowledges that Omnistrate may update or modify its Security Measures to reflect technical progress and development, provided that such updates do not result in a degradation of the overall security of the Services purchased by the Customer. Omnistrate will maintain its SOC 2 Type II certification or equivalent industry-recognized standards to demonstrate continued compliance with its security commitments.

6.3 Personnel. Omnistrate restricts its personnel from processing Customer Personal Data without authorization by Omnistrate as set forth in the Security Measures and shall ensure that any person who is authorized by Omnistrate to process Customer Personal Data is under an appropriate obligation of confidentiality and agrees to comply with applicable Data Protection Laws.

6.4 Customer Responsibilities. Without prejudice to Omnistrate's obligations under this DPA, and elsewhere in the Agreement, Customer agrees that, without limitation of Omnistrate's obligations under this Section 6, Customer is solely responsible for its use of the Services, including (i)making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; and (ii) protecting and securing account authentication credentials, systems, and devices Customer Personal Data; (iii) protecting the security of Customer Personal Data when in transit to and from the Services; (iv) implementing measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (iv) taking any appropriate steps to securely encrypt or pseudonymise any Customer Personal Data uploaded to the Services. Without limiting Omnistrate's obligations hereunder, Customer is responsible for reviewing the information made available by Omnistrate relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6.5 Security Incident. In the event of a Security Incident, Omnistrate will notify Customer without undue delay and in any event within seventy-two (72) hours after becoming aware of facts reasonably indicating that a Security Incident affecting Customer Personal Data has occurred, and will provide updates to Customer. Omnistrate will reasonably cooperate with Customer as required to fulfil Customer's obligations under Data Protection Laws. Omnistrate shall take reasonable steps to identify the cause of such Security Incident, minimize harm, and prevent a recurrence. Omnistrate will take reasonable steps to provide Customer with information available to Omnistrate that Customer may reasonably require to comply with its obligations under Data Protection Laws. Omnistrate's notification of or response to a Security Incident under this Section 6.5 will not be construed as an acknowledgement by Omnistrate of any fault or liability with respect to the Security Incident.

6.6 De-identified Data: With respect to any de-identified data received/created by Omnistrate from Customer Personal Data, Omnistrate will: (i) take any necessary measures to ensure that such de-identified data remains to de-identified and shall not be re-identified; (ii) comply with the requirements of Data Protection Laws with respect to such de-identified data; and (iv) contractually obligate any recipients of the de-identified data to comply with restrictions substantially similar to those set forth in this Section 6.6.

7. Audits

7.1 Customer Audit Rights. To the extent Customer's audit requirements under applicable Data Protection Laws cannot reasonably be satisfied through Omnistrate's relevant audit reports and certifications ("**Audit Reports**"), documentation or compliance information Omnistrate makes generally available to its customers or through reasonably written audit questions, which Customer may request no more than once per calendar year, Omnistrate will promptly respond to Customer's additional audit requests. Before the commencement of an audit, Customer and Omnistrate will mutually agree upon the scope, timing, duration, and control and evidence requirements, provided that this requirement to agree will not permit Omnistrate to unreasonably delay performance of the audit. To the extent needed to perform the audit, Omnistrate will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Personal Data by Omnistrate available, provided Customer or any third- party authorized auditor complies with Omnistrate's standard safety, confidentiality, and security policies or procedures in conducting any such audits. Neither Customer nor the third-party auditors, if any, shall have access to any data from Omnistrate's other customers or to Omnistrate systems or facilities not involved in the processing of Customer Personal Data. Customer is responsible for all costs and expenses related to such audits, including any reasonable costs and expenses that Omnistrate expends for any such audit.

7.2 Results of Audits. Customer will promptly notify Omnistrate of any non-compliance discovered during the course of an audit and provide Omnistrate any reports generated in connection with any audit under this Section, unless prohibited by Data Protection Laws or otherwise instructed by a Supervisory Authority. Customer may use the audit reports solely for the purposes of meeting Customer's audit requirements under Data Protection Laws to confirm that Omnistrate's Processing of Customer Personal Data complies with this DPA.

8. Return or Deletion of Data

Return or Deletion of Data. Upon termination or expiration of the Agreement, Omnistrate shall, at Customer's election, delete or return all Customer Personal Data in its possession or control in accordance with the terms of the Agreement. Upon Customer's written request, Omnistrate will certify in writing that such deletion has been completed in accordance with this Section 8.. Customer Personal Data contained in backup or archival systems may be retained until deleted or overwritten in the ordinary course pursuant to Omnistrate's standard backup retention procedures, provided that such retained data remains subject to the confidentiality and security obligations of this DPA and is not accessed or used except as necessary for disaster recovery, security, or compliance with applicable law.

9. Cooperation

9.1 Data Subject Request. The Services provide Customer with the ability to retrieve and delete Customer Personal Data. Customer may use these controls to comply with Customer's

obligations under applicable Data Protection Laws, including Customer's obligations related to any requests from data subjects involving Customer Personal Data ("**Data Subject Requests**"). To the extent that Customer is unable to independently access the relevant Customer Personal Data using such controls or otherwise, Omnistrate shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to such Data Subject Requests. In the event that any such Data Subject Request is made directly to Omnistrate, Omnistrate shall, to the extent legally permitted: (i) advise the data subject to submit their Data Subject Request to Customer; (ii) promptly notify Customer; and (iii) not otherwise respond to that Data Subject Request without authorization from Customer unless legally compelled to do so. Customer will be responsible for responding to any such Data Subject Requests.

9.2 Requests for Customer Personal Data. If Omnistrate receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Personal Data, Omnistrate shall, to the extent permitted by applicable laws, promptly notify Customer in writing of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

9.3 Legal Compliance. To the extent Omnistrate is required under applicable Data Protection Laws, Omnistrate will (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

10. CCPA Compliance

10.1 Applicability. This section 10 applies to the extent Customer is a Business that is subject to the CCPA and submits Personal Information (as that term is defined under CCPA) as part of Customer Personal Data in connection with Omnistrate's performance of the Agreement. Customer appoints Omnistrate as its Service Provider to collect and process the Customer Personal Data for the purposes outlined in section 3.4

10.2 Service Provider Commitments. Omnistrate will not (a) Sell or share Customer Personal Data; (b) retain, use, or disclose the Customer Personal Data for any purpose other than for the Business Purpose, including to retain, use, or disclose the Customer Personal Data for a commercial purpose other than providing its Services under the Agreement; (c) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Omnistrate and the Customer; (d) process the Customer Personal Data for targeted and/or cross context behavioural advertising; (e) combine Customer Personal Data that it receives from, or on behalf of, Customer, with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Consumer, if and to the extent such combination would be inconsistent with the limitations on Service Providers under the CCPA or other laws. Omnistrate will comply with applicable obligations under the CCPA and provide the same level of privacy protection to Personal Information as is required by the CCPA. The Customer has the right to take reasonable and appropriate steps to help ensure that Omnistrate uses the Personal Information transferred in a manner consistent with Customer's obligations under the CCPA by exercising Customer's audit rights in Section 7. Omnistrate will notify Customer if it makes a determination that Omnistrate can no longer meet its obligations under the CCPA

11. General

11.1 For the avoidance of doubt, any claim or remedies the Customer and/or its Affiliates may have against Omnistrate, any of its Affiliates and their respective employees, agents and Sub processors (hereinafter "**Omnistrate Group**") arising under or in connection with this DPA, including: (i) for breach of this DPA;

(ii) for breach of cross-border data transfers and related provisions outlined in the Standard Contractual Clauses (to the extent applicable and as defined in Exhibit A hereto); (iii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iv) under applicable Data Protection Laws, including any claims relating to damages paid to a data subject, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Such limitation of liability does not apply to any direct claim or remedies a data subject may have against Customer or Omnistrate. Customer further agrees to indemnify Omnistrate in the event of any regulatory penalties incurred by Omnistrate Group in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws, subject to the limitations of liability set forth in the Agreement.

11.2 Any claims against Omnistrate or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

11.3 To the extent reasonably necessary to comply with changes to applicable Data Protection Laws or in response to guidance or mandates issued by any court, regulatory body, or supervisory authority with jurisdiction over Omnistrate, Omnistrate may modify, amend, or supplement the terms of this DPA, provided that any such modification will not materially reduce the level of protection afforded to Customer Personal Data under this DPA. Omnistrate will make reasonable efforts to provide prior notice of any such changes to the Customer via email, on Omnistrate's website, and/or in the Omnistrate portal, where applicable.

11.4 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.5 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in Exhibit A (Cross-Border Data Transfers); (2) the terms of this DPA outside of Exhibit A; and (3) the Agreement. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

11.6 If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

EXHIBIT A

CROSS-BORDER DATA TRANSFERS

1. Definitions

(a) "**EU Standard Contractual Clauses (Controller-to-Processor)**" or **"EU SCCs (Controller-to-Processor)"** means the terms located at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914

(b) "**EU Standard Contractual Clauses (Processor-to-Processor)**" or **"EU SCCs (Processor-to-Processor)"** means the terms located at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914

(c) "**UK Addendum"** means the terms located in EXHIBIT B

2. EU Standard Contractual Clauses

2.1. For transfers of Customer Personal Data from the EEA and/or Switzerland that are subject to Section 4.2 of the DPA:

(a) Where Customer is a controller of Customer Personal Data, the EU SCCs (Controller-to-Processor) will apply and are incorporated into the DPA by reference; and

(b) Where Customer is a processor of Customer Personal Data, the EU SCCs (Processor-to-Processor) will apply and are incorporated into the DPA by reference.

3. UK Addendum

3.1. For transfers of Customer Personal Data from the United Kingdom that are subject to Section 4.2 of the DPA, the UK Addendum will apply and are incorporated into the DPA by reference.

4. Alternative Data Export Solutions

4.1. Notwithstanding the foregoing, the parties agree that in the event Omnistrate adopts another alternative data export solution (as recognized under applicable Data Protection Laws), then the alternative data export solution shall apply instead of the Standard Contractual Clauses. In the event that the alternative data export solution is later determined to not constitute an adequate level of data protection under applicable Data Protection Laws, the Standard Contractual Clauses shall apply as the data export solution.

EXHIBIT B

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES ("UK ADDENDUM")

Capitalized terms used but not defined in this UK Addendum have the meanings given to them in the Master Services Agreement or other written or electronic terms of service or subscription agreement ("Agreement") and/or respective data processing agreement ("DPA") into which this UK Addendum is incorporated.

This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

Table 1: Parties

Start Date	Date of commencement of the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer**
Parties' details	**Full Legal Name:** Legal entity identified as "Customer" in the DPA **Main address:** As specified in the Agreement, DPA and/or Order Form	**Full Legal Name:** Omnistrate Inc., **Main address:** 541 Jefferson Ave, Suite 100, Redwood City, CA 94063
Key Contact	**Job Title:** Customer's account owner **Contact Details:** Customer's account owner telephone and e-mail address, or the email address for which Customer elects to receive legal communications	**Job Title:** Omnistrate Legal **Contact Details:** legal@omnistrate.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The versions of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information (together referred to as "Omnistrate EU SCCs"): ● EU Standard Contractual Clauses (Module 2 - Controller-to-Processor) available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914 ● EU Standard Contractual Clauses (Module 3 Processor-to-Processor) available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties	See Table 1 Parties in this Addendum.
Annex 1B: Description of Transfer	See section 3.5 and section 4 in this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	See Section 6.1 in this DPA
Annex III: List of Sub-processors	See EXHIBIT C

PART 2: MANDATORY CLAUSES

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 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

EXHIBIT C

OMNISTRATE SUBPROCESSORS

Omnistrate uses certain Sub-processors to assist in providing the Services. A Sub-processor is a third-party company engaged by Omnistrate to process Personal Data (i) on behalf of Omnistrate's customers; (ii) in accordance with Customer's instructions as communicated by Omnistrate; and (iii) in strict accordance with the terms of a written contract between Omnistrate and the Sub-processor. Omnistrate has entered into Standard Contractual Clauses with its Sub-processors, which is the legal basis for applicable cross-border data transfers.

A. Infrastructure Providers

Omnistrate Platform runs on top of the infrastructure provider selected by Customer. The cloud providers outlined below may host Customer Personal Data:

Sub-Processor	Purpose	Corporate Location	Data Subjects	Storage Location
Amazon Web Services, Inc.	Infrastructure hosting, data storage, and backups.	United States	Customer's customers, employees, contractors, suppliers, and other third parties.	United States and as selected by customer.
Google LLC (Google Cloud Platform)	Cloud infrastructure, application hosting, and services.	United States	Customer's customers, employees, contractors, suppliers, and other third parties.	As selected by customer.
Microsoft Corporation (Azure)	Cloud infrastructure, application hosting, and services.	United States	Customer's customers, employees, contractors, suppliers, and other third parties.	As selected by customer.

B. Other Third-Party Sub-processors

While Omnistrate will never ask you to do so, in the unlikely event you provide Customer Personal Data as part of a support request, Omnistrate also engages the following entities which may have access to or process Customer Personal Data:

Sub-Processor	Purpose	Corporate Location	Data Subjects
Slack Technologies, LLC.	Customer support	United States	Customer's employees and contractors
Zendesk, Inc.	Customer support	United States	Customer's customers, employees and contractors
Raintank Inc., dba Grafana Labs	Logging, monitoring, and metrics visualization	United States	Customer's customers, employees and contractors

Stripe, Inc.	Payment processing	United States	Customer's customers, employees and contractors

C. Affiliates

The following entities are Omnistrate Affiliates. They may function as Sub-processors to provide the Services and related support to the extent respective restricted employees have access to Customer Personal Data.

Sub-Processor	Corporate Location	Data Subjects
Omnistrate India Private Limited	India	Customer's customers, employees, contractors, suppliers, and other third parties.