



MANTLE

www.hey mantle.com

MANTLE REVOPS INC

424-Warmstone Drive, Stittsville ON K2S 0W2
(613) 866-4931 | team@hey mantle.com

Mantle's Data Processing Addendum

This Data Processing Addendum ("*Addendum*"), applies to agreements between Mantle RevOps Inc., a Canadian corporation ("*Mantle*") and entities who use Mantle's services and who are subject to Applicable Law ("*User*", and collectively with Mantle, the "*Parties*"), and sets forth the terms of use relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Mantle to User pursuant to the terms of service's agreement entered into between the Parties available on the Mantle website, hey mantle.com/tos, (the "*Terms of Use*"). Mantle may update these terms from time to time in its sole discretion.

The Addendum is made available at hey mantle.com/dpa. For Users that would like to receive a signed copy of the Mantle Addendum, please complete the form available at hey mantle.com/dpa and submit the signed Addendum to legal@hey mantle.com. No changes made to this copy are agreed to by Mantle or its affiliates.

1. Definitions

- a. "*Applicable Law*" means all applicable European Union ("EU") or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR"), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; the EU Directive 2002/58/EC ("e-Privacy Directive"), as replaced from time to time, and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications.
- b. "*Data Controller*" means a person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
- c. "Data Privacy Framework (DPF)" means the EU-U.S. Data Privacy Framework approved by the European Commission on July 10, 2023, which provides a legal mechanism for transferring personal data from the EU to certified U.S. organizations under Article 45 of the GDPR.
- d. "*Data Processor*" means a person who Processes Personal Data on behalf of the Data Controller.
- e. "*Data Security Measures*" means technical and organizational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorized access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.
- f. "*Data Subject*" means an identified or identifiable natural person to which the Personal Data pertain.
- g. "*Instructions*" means the Terms of Use, this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.
- h. "*Personal Data*" means any information relating to an identified or identifiable natural person Processed by Mantle in accordance with User's Instructions pursuant to this Addendum; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical,



physiological, genetic, mental, economic, cultural or social identity of that natural person.

i. “*Personal Data Breach*” a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

j. “*Process*”, “*Processed*”, or “*Processing*” means any operation or set of operations performed upon 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. “*Services*” means the services offered by Mantle and used by User under the Terms of Use.

l. “*Sub-Processor*” means the entity engaged by the Data Processor or any further Sub-Processor to Process Personal Data on behalf and under the authority of the Data Controller.

2. Roles and Responsibilities of the Parties

a. The Parties acknowledge and agree that User is acting as a Data Controller, and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data Processed under this Addendum, and Mantle is acting as a Data Processor on behalf and under the Instructions of User.

b. Any Personal Data will at all times be and remain the sole property of User and Mantle will not have or obtain any rights therein.

3. Obligation of the Mantle

Mantle agrees and warrants to:

a. Process Personal Data disclosed to it by User only on behalf of and in accordance with the Instructions of the Data Controller and Annex 1 of this Addendum, unless Mantle is otherwise required by Applicable Law, in which case Mantle shall inform User of that legal requirement before Processing the Personal Data, unless informing the User is prohibited by law. Mantle shall immediately inform User if, in Mantle’s opinion, an Instruction provided infringes Applicable Law.

b. Ensure that any person authorized by Mantle to Process Personal Data in the context of the Services is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Data Controller.

c. Mantle shall enter into any written agreements as are necessary in User’s reasonable determination, including without limitation the Standard Contractual Clauses (as issued under the European Commission Decision of 4 June 2021) and the UK Addendum to the European Commission Standard Contractual Clauses (as issued by the Information Commissioner’s Office under or pursuant to section 119A(1) of the Data Protection Act 2018), to comply with Applicable Law concerning any cross-border transfer of Personal Data, whether to or from Mantle.

d. Inform User promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and not respond to such requests, unless instructed by the



MANTLE

www.hey mantle.com

MANTLE REVOPS INC

424-Warmstone Drive, Stittsville ON K2S 0W2
(613) 866-4931 | team@hey mantle.com

User in writing to do so. Taking into account the nature of the Processing of Personal Data, Mantle shall assist User, by appropriate technical and organizational measures, insofar as possible, in fulfilling User's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data.

e. Notify User immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. User shall have the right to defend such action in lieu of and on behalf of Mantle. User may, if it so chooses, seek a protective order.

f. Maintain internal record(s) of Processing activities, copies of which shall be provided to User by Mantle or to supervisory authorities upon request. Such records must contain at least: (i) the name and contact details of Mantle; (ii) the categories of Processing activities carried out under this Addendum; (iii) information on data transfers to a third country or a third party, where applicable; and (iv) a general description of the Data Security Measures implemented to protect Personal Data Processed under this Addendum.

g. Mantle retains operational and security logs, including authentication, access, and error logs, for a period of **14 days**, unless a longer retention period is required by law or necessary for the investigation of specific incidents. After this period, logs are securely deleted or anonymized in accordance with industry standards.

4. Sub-Processing

a. Mantle shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless Mantle has entered into a written agreement with each such third party that imposes obligations on the third party that are equivalent to those imposed on Mantle under this Addendum. Mantle shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data.

b. Mantle engages sub-processors, including Amazon Web Services (AWS) for cloud infrastructure and data storage; SendGrid (Twilio) for transactional and customer-initiated email delivery; Cloudflare for content delivery and protection; Google Workspace for email-based customer communications; Stripe for payment processing; Elasticsearch (Elastic NV) for user event and activity indexing; Confluent for real-time event streaming; Plain.com for customer support communications; and Slack Technologies for customer chat and support. Where applicable, these sub-processors are certified under the EU-U.S. Data Privacy Framework (DPF), providing appropriate safeguards for cross-border data transfers to the United States.

c. The Subprocessors currently engaged by Mantle which may process Personal Data on Mantle's behalf are set out in Annex 1. Mantle shall notify User in writing in the event that Mantle proposes to add any additional Sub-Processors.

5. Compliance with Applicable Laws

a. Each Party covenants and undertakes to the other that it shall comply with all Applicable Laws in the use of the Services.

b. As between the parties, Subscriber is responsible for the lawfulness of the Processing of the Subscriber Personal Data. Subscriber will not use the Services in conjunction with Personal Data to the extent that doing so would violate applicable Data Protection Laws.

c. Mantle shall in good faith negotiate any further data Processing agreement reasonably requested by User for purposes of compliance with the Applicable Law. In case of any conflict between this



MANTLE

www.hey mantle.com

MANTLE REVOPS INC

424-Warmstone Drive, Stittsville ON K2S 0W2
(613) 866-4931 | team@hey mantle.com

Addendum and the Terms of Use, this Addendum shall prevail with regard to the Processing of Personal Data covered by it.

6. Data Security

a. Mantle shall develop, maintain and implement a written information security program that complies with Applicable Law and good industry practice. Mantle's information security program shall include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:

- i. The encryption of Personal Data in transit.
- ii. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- iii. The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and
- iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures adopted pursuant to this provision for ensuring the security of the Processing.

b. Mantle shall supervise Mantle personnel to the extent required to maintain appropriate privacy, confidentiality and security of Personal Data. Mantle shall provide training, as appropriate, regarding the privacy, confidentiality and information security requirements set forth in this Addendum to all Mantle personnel who have access to Personal Data.

c. Promptly upon the expiration or earlier termination of the Terms of Use, or such earlier time as User requests, Mantle shall securely destroy or render unreadable or indecipherable, each and every original and copy in every media of all Personal Data in Mantle's, its affiliates' or their respective subcontractors' possession, custody or control. In the event applicable law does not permit Mantle to comply with the destruction of the Personal Data, Mantle warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum other than to the extent.

7. Data Breach Notification

Mantle shall without undue delay inform User in writing of any Personal Data Breach of which Mantle becomes aware, but in no case longer than seventy-two (72) hours after it becomes aware of the Personal Data Breach. The notification to User shall include all available information regarding such Personal Data Breach, including information on:

- a) The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;
- b) The likely consequences of the Personal Data Breach; and
- c) The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Mantle shall promptly take all necessary and advisable corrective actions, and shall cooperate with User in



MANTLE

www.hey mantle.com

MANTLE REVOPS INC

424-Warmstone Drive, Stittsville ON K2S 0W2

(613) 866-4931 | team@hey mantle.com

reasonable and lawful efforts to prevent, mitigate or rectify such Breach. Mantle shall provide such assistance as required to enable User to satisfy User's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR.

8. Audit

Mantle shall on written request (but not more than once per year, other than in the event of a breach) make available to User all information necessary to demonstrate compliance with the obligations set forth in this Addendum and, at the User's expense, allow for and contribute to audits, including inspections, conducted by User or another auditor mandated by User. Upon prior written request by User (provided that it shall be not more than once per year other than in the event of a breach), Mantle agrees to cooperate and, within reasonable time, provide User with: (a) audit reports and all information necessary to demonstrate Mantle's compliance with the obligations laid down in this Addendum; and (b) confirmation that the audit has not revealed any material vulnerability in Mantle's systems, or to the extent that any such vulnerability was detected, that Mantle has fully remedied such vulnerability. Mantle's failure to comply with this obligation shall entitle User to suspend the Processing of Personal Data Processed by Mantle, and to terminate any further Processing of Personal Data, this Addendum and/or the Terms of Use, if doing so is required to comply with Applicable Law.

9. CCPA

The Parties agree and acknowledge that, as Mantle processes personal information on behalf of User in providing the Services Mantle is considered be a service provider for User under the CCPA. Mantle acknowledges and agrees that it may not retain, use, or disclose personal information made available to it by User for any purpose, including commercial purposes, other than in connection with performing the Services; and Mantle not sell such personal information.

10. Governing Law

To the extent required by Applicable Law, this Addendum shall be governed by the law of the Province of Ontario, Canada. In all other cases, this Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

IN WITNESS WHEREOF, the Parties, but their authorized representatives, have executed this Addendum.

MANTLE RevOps INC

USER: _____

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____



ANNEX 1: SCOPE OF THE DATA PROCESSING

SCOPE OF THE DATA PROCESSING

This Annex forms part of the Data Processing Addendum between User and Mantle.

The Processing of Personal Data concerns the following categories of Data Subjects:

1. Users of the Mantle platform (e.g., customer employees, administrators, or team members); and
2. Individuals whose information is provided to Mantle through onboarding, billing, support, or integrations

The Processing concerns the following categories of Personal Data:

Name, Email address, Login credentials (e.g., username, password), IP address and device/browser information, Profile details (if provided), Platform usage data (e.g., features used, login times), Support messages or customer inquiries, Billing contact information

The Processing concerns the following categories of Sensitive Data:

Mantle does not intentionally collect or process sensitive personal data as defined in Article 9 of the GDPR, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, health information, or data concerning a person's sex life or sexual orientation.

If users voluntarily submit such data (e.g., in a support message or profile field), it is not required, and Mantle does not actively use or analyze such data as part of its services.

The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):

1. To provide and maintain the Mantle platform and services
2. To authenticate users and manage account access
3. To monitor usage and ensure platform security and performance
4. To support customer inquiries and resolve technical issues
5. To facilitate onboarding, billing, and service-related communications



Mantle uses the following Sub-Processors:

Sub-Processor	Purpose / Processing Activity	Location	Safeguards / DPF Status
Infrastructure and Hosting			
Amazon Web Services (AWS)	Cloud infrastructure and data storage	USA	DPF Certified
Cloudflare	CDN, web performance, and security services (e.g., DDoS)	USA	DPF Certified
Confluent	Real-time data streaming and processing infrastructure	USA	SCCs in place
Elasticsearch (Elastic NV)	Search indexing and analytics involving user event data	USA	DPF Certified
Communication and Collaboration			
SendGrid (Twilio)	Transactional and in-app email delivery	USA	DPF Certified
Google Workspace (Google LLC)	Customer communication via email	USA	DPF Certified
Plain.com	Customer support communications and case management	UK	SCCs in place
Slack Technologies	Customer chat and support communications	USA	DPF Certified
Mailchimp (Intuit Inc.)	Marketing email campaigns to users and customers	USA	DPF Certified
Payments			
Stripe	Payment processing	USA	DPF Certified



ANNEX II
STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Where the transfer of Personal Data to Mantle is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses (SCCs), which shall be deemed incorporated into and form part of the Terms as follows:
 - a. In relation to transfers of Personal Data protected by the EU GDPR, the SCCs shall apply as follows:
 - I. Module Two terms shall apply (where Customer is the controller of Personal Data) and the Module Three terms shall apply (where Customer is the processor of Personal Data);
 - II. in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede the SCCs under the same terms and conditions as Customer, subject to mutual agreement of the parties;
 - III. in Clause 9, option 2 (“general authorization”) is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in the DPA
 - IV. in Clause 11, the optional language shall not apply;
 - V. in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;
 - VI. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
 - VII. Annex I shall be deemed completed with the information set out in Annex A to the Terms; and
 - VIII. Annex II shall be deemed completed with the information set out in the applicable security policies, subject to Section 16 (Data Security) of the Terms of Service.
 - b. In relation to transfers of Personal Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:
 - I. the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the Terms;
 - II. Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A and Annex B to the Terms and applicable security policies respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting “neither party”; and
 - III. any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.
 - c. In relation to transfers of Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:
 - I. references to “Regulation (EU) 2016/679” and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;
 - II. references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “Switzerland” and/or “Swiss law” (as applicable);
 - III. references to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection Information Commissioner” and “applicable courts of Switzerland”;
 - IV. the SCCs shall be governed by the laws of Switzerland ; and
 - V. disputes shall be resolved before the competent Swiss courts.
2. Where the Standard Contractual Clauses apply, this section sets out the parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:
 - a. where Customer is itself a processor of Personal Data acting on behalf of a third party controller and Mantle would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Mantle may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;



MANTLE

www.hey mantle.com

MANTLE REVOPS INC

424-Warmstone Drive, Stittsville ON K2S 0W2
(613) 866-4931 | team@hey mantle.com

-
- b. the certification of deletion described in Clause 16(d) of the SCCs shall be provided by Mantle to Customer upon Customer's written request;
 - c. for the purposes of Clause 15(1)(a) the SCCs, Mantle shall notify Customer and not the relevant data subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant data subjects as necessary; and
 - d. taking into account the nature of the processing, Customer agrees that it is unlikely that Mantle would become aware of Personal Data processed by Mantle is inaccurate or outdated. To the extent Mantle becomes aware of such inaccurate or outdated data, Mantle will inform the Customer in accordance with Clause 8.4 of the SCCs.
 - e. Mantle has conducted Transfer Impact Assessments (TIAs) where applicable, in accordance with GDPR and EDPB guidelines, to assess the legal environment and risks related to cross-border data transfers relying on Standard Contractual Clauses.