Data Processing Agreement

PREPARED BY RMS CLOUD

DECEMBER 2022

RMS

DATA PROCESSING AGREEMENT

This Data Processing Addendum ("DPA") is incorporated into, and is subject to the terms and conditions of, the Agreement between RMS Cloud (together with its Affiliates) and the customer entity that is a party to the Agreement ("Customer" or "you").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA (including the SCCs (where applicable), as defined herein).

1. DEFINITIONS

"Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"Agreement" means RMS Cloud Standard Terms of and Conditions, or other written or electronic agreement, which govern the provision of the Service to Customer, as such terms or agreement may be updated from time to time.

"Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

"Customer Data" means any personal data that RMS Cloud processes on behalf of Customer via the Service, as more particularly described in this DPA.

"Data Protection Laws" means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, European Data Protection Laws and Non-European Data Protection Laws.

“European Data Protection Laws” means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (“GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); (iv) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, “UK Data Protection Laws”); and (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance (“Swiss DPA”).

“Europe” means, for the purposes of this DPA, the European Economic Area and its member states (“EEA”), Switzerland and the United Kingdom (“UK”).

“Non-European Data Protection Laws” includes the California Consumer Privacy Act (“CCPA”); the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”); the Privacy Act 1988 (Cth) of Australia, as amended (“Australian Privacy Law”). the Data Protection Laws and Regulations Singapore 2022 (“Singapore Privacy Law)”, Privacy Act 2020 of New Zealand (“New Zealand Privacy Law”)

“SCCs” means either (i) the standard contractual clauses between controllers and processors adopted by the European Commission in its Implementing Decision 2010/87/EU of 5 February 2010, and currently located here (the “2010 Controller-to-Processor Clauses”); (ii) the standard contractual clauses between controllers and processors adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021, and currently located here (the “2021 Controller-to-Processor Clauses”); or (iii) the standard contractual clauses between processors adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021, and currently located here (the “2021 Processor-to-Processor Clauses”); as applicable in accordance with Section 6.3.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by RMS Cloud.

“Sensitive Data” means (a) social security number, tax file number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of “special categories of data” under applicable Data Protection Laws.

“Sub-processor” means any processor engaged by RMS Cloud or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of RMS Cloud but shall exclude RMS Cloud employees, contractors, or consultants.

The terms “personal data”, “controller”, “data subject”, “processor” and “processing” shall have the meaning given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and “process”, “processes” and “processed”, with respect to any Customer data, shall be interpreted accordingly.

2. ROLES AND RESPONSIBILITIES

2.1 Parties’ roles. If European Data Protection Laws applies to either party’s processing of Customer Data, the parties acknowledge and agree that with regard to the processing of Customer Data, RMS Cloud is a processor acting on behalf of Customer (whether itself a controller or a processor).

2.2 Purpose limitation. RMS Cloud shall process Customer Data only in accordance with Customer’s documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing (“Permitted Purposes”). The parties agree that the Agreement, including this DPA, along with the Customer’s configuration of or use of any settings, features, or options in the Service (as the Customer may be able to modify from time to time) constitute the Customer’s complete and final instructions to RMS Cloud in relation to the processing of Customer Data (including for the purposes of the SCCs), and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 Prohibited data. Customer will not provide (or cause to be provided) any Sensitive Data to RMS Cloud for processing under the Agreement, and RMS Cloud will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.4 Customer compliance. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Customer Data and any processing instructions it issues to RMS Cloud; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for RMS Cloud to process Customer Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any content created, sent, or managed through the Service, including those relating to obtaining consents (where required) to send emails or other messaging, the content of the emails or other messaging and its email or other messaging deployment practices.

2.5 Lawfulness of Customer's instructions. Customer will ensure that RMS Cloud's processing of the Customer Data in accordance with Customer's instructions will not cause RMS Cloud to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. RMS Cloud shall promptly notify Customer in writing, unless prohibited from doing so under European Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates European Data Protection Laws. Customer shall serve as the sole point of contact for RMS Cloud and RMS Cloud need not interact directly with (including to provide notifications to or seek authorization from) any third-party controller other than through regular provision of the Service to the extent required under the Agreement. Customer shall be responsible for forwarding any notifications received under this DPA to the relevant controller, where appropriate.

3. SUB-PROCESSING

3.1 Authorized Sub-processors. Customer agrees that RMS Cloud may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by RMS Cloud and authorized by Customer are available at https://www.rmscloud.com/terms-and-conditions . RMS Cloud RMS will notify the Customer in advance of any changes to Subprocessors. Within 30 days of such notification, the Customer can object to the change on the basis that such change would cause the Customer to violate applicable legal requirements. The Customer's objections must be in writing and contain specific reasons for its objection and options to mitigate, if any. If the Customer does not object within the 30 days of such notification RMS shall be entitled to proceed with the change.

3.2 Sub-processor obligations. RMS Cloud shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause RMS Cloud to breach any of its obligations under this DPA. Customer acknowledges and agrees that, where applicable, RMS Cloud fulfills its obligations under Clause 9 of the 2021 Controller-to-Processor Clauses and 2021 Processor-to-Processor Clauses (as applicable) by complying with this Section 3 and that RMS Cloud may be prevented from disclosing Sub-processor agreements to Customer due to confidentiality restrictions but RMS Cloud shall, upon request, use reasonable efforts to provide Customer with all relevant information it reasonably can in connection with Subprocessor agreements.

4. SECURITY

4.1 Security Measures. RMS Cloud shall implement and maintain appropriate technical and organizational security measures that are designed to protect Customer Data from Security Incidents and designed to preserve the security and confidentiality of Customer Data in accordance with RMS Cloud's security standards.

4.2 Confidentiality of processing. RMS Cloud shall ensure that any person who is authorized by RMS Cloud to process Customer Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 Updates to Security Measures. Customer is responsible for reviewing the information made available by RMS Cloud relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that RMS Cloud may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

4.4 Security Incident response. Upon becoming aware of a Security Incident, RMS Cloud shall: (i) notify Customer without undue delayafter becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. RMS Cloud's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by RMS Cloud of any fault or liability with respect to the Security Incident.

4.5 Customer responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials.

5. SECURITY INFORMATION REQUESTS

5.1 RMS Cloud shall respond to all reasonable requests for information made by Customer to confirm RMS Cloud's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to privacy@rmscloud.com, provided that Customer shall not exercise this right more than once per calendar year.

6. INTERNATIONAL TRANSFERS

6.1 Data center locations. Subject to Section 6.2, Customer acknowledges that RMS Cloud may transfer and process Customer Data to and in Australia and anywhere else in the world where RMS Cloud, its Affiliates or its Sub-processors maintain data processing operations. RMS Cloud shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

6.2 Australian data. To the extent that RMS Cloud is a recipient of Customer Data protected by the Australian Privacy Law, the parties acknowledge and agree that RMS Cloud may transfer such Customer Data outside of Australia as permitted by the terms agreed upon by the parties and subject to RMS Cloud complying with this DPA and the Australian Privacy Law.

6.3 European Data transfers. To the extent that RMS Cloud is a recipient of Customer Data protected by European Data Protection Laws ("European Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for personal data (as described in applicable European Data Protection Laws), the parties agree to abide by and process European Data in compliance with the SCCs, which shall be incorporated into and form an integral part of this DPA as follows:

- (a) if Customer started using the Service before 27 September 2021, the 2010 Controller-to-Processor Clauses shall apply (regardless of whether Customer is a controller or a processor) until December 27, 2022, and thereafter the 2021 Controller-to-Processor Clauses and/or the 2021 Processor-to-Processor Clauses shall automatically apply (according to whether Customer is a controller and/or a processor) thereafter;

- (b) if Customer started using the Service on or after 27 September 2021, the 2021 Controller-to-Processor Clauses and/or the 2021 Processor-to-Processor Clauses shall apply (according to whether Customer is a controller and/or a processor) immediately.

6.4 Compliance with the SCCs. The parties agree that if RMS Cloud cannot ensure compliance with the SCCs, it shall promptly inform Customer of its inability to comply. If Customer intends to suspend the transfer of European Data and/or terminate the affected parts of the Service, it shall first provide notice to RMS Cloud and provide RMS Cloud with a reasonable period of time to cure such non-compliance, during which time RMS Cloud and Customer shall reasonably cooperate to agree what additional safeguards or measures, if any, may be reasonably required. Customer shall only be entitled to suspend the transfer of data and/or terminate the affected parts of the Service for non-compliance with the SCCs if RMS Cloud has not or cannot cure the non-compliance within a reasonable period.

6.5 Alternative transfer mechanism. To extent that and for so long as the SCCs as implemented in accordance with Section 6.3 cannot be relied on to lawfully transfer personal data in compliance with UK Data Protection Laws, the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs") shall be incorporated by reference and deemed completed with the relevant applicable information. Additionally, to the extent RMS Cloud adopts an alternative lawful data transfer mechanism for the transfer of European Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Laws and extends to the countries to which European Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer European Data (within the meaning of applicable European Data Protection Laws), RMS Cloud may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of European Data.

7. RETURN OR DELETION OF DATA

Deletion or return on termination. Upon termination or expiration of the Agreement, RMS Cloud shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, except that this requirement shall not apply to the extent RMS Cloud is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data RMS Cloud shall securely isolate, protect from any further processing and eventually delete in accordance with RMS Cloud's deletion policies, except to the extent required by applicable law. The parties agree that the certification of deletion of Customer Data described in Clause 8.5 and 16(d) of the 2021 Controller-to-Processor Clauses and 2021 Processor-to-Processor Clauses (as applicable) shall be provided by RMS Cloud to Customer only upon Customer's written request.

8. DATA SUBJECT RIGHTS AND COOPERATION

8.1 Data subject requests. As part of the Service, RMS Cloud provides Customer with a number of self-service features, that Customer may use to retrieve, correct, delete, or restrict the use of Customer Data, which Customer may use to assist it in connection with its (or its third-party controller's) obligations under the Data Protection Laws with respect to responding to requests from data subjects via Customer's account at no additional cost. In addition, RMS Cloud shall, considering the nature of the processing, provide reasonable additional assistance to Customer to the extent possible to enable Customer (or its third-party controller) to comply with its data protection obligations with respect to data subject rights under Data Protection Laws. In the event that any such request is made to RMS Cloud directly, RMS Cloud shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Customer) or legally required, without Customer's prior authorization. If RMS Cloud is required to respond to such a request, RMS Cloud shall, where the Customer is identified or identifiable from the request, promptly notify Customer and provide Customer with a copy of the request unless RMS Cloud is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent RMS Cloud from responding to any data subject or data protection authority requests in relation to personal data for which RMS Cloud is a controller.

8.2 Data protection impact assessment. To the extent required under applicable Data Protection Laws, RMS Cloud shall (considering the nature of the processing and the information available to RMS Cloud) provide all reasonably requested information regarding the Service to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. RMS Cloud shall comply with the foregoing by: (i) complying with Section 5 (Security); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

9. LIMITATION OF LIABILITY

10.1 Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.2 Any claims made against RMS Cloud or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

10. RELATIONSHIP WITH THE AGREEMENT

10.1 This DPA shall remain in effect for as long as RMS Cloud carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement.

10.2 The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service.

10.3 In the event of any conflict or inconsistency between this DPA and the Standard Terms of Use, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Standard Terms of Use.

10.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

10.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

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

Effective December 27, 2022

– END –