METOLIUS, LLC

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated into, and supplements, the agreement(s) between Metolius, LLC ("**Metolius**") and Customer governing Metolius's provision, and Customer's receipt of the Services (collectively, the "**Agreement**").

This DPA is an agreement between Metolius and the entity who receives the Services from Metolius pursuant to an Agreement that incorporates this DPA ("**Customer**") and is effective as of the date this DPA is incorporated into such Agreement (the "**DPA Effective Date**"). Customer and Metolius are each referred to herein as a "**Party**" and collectively as the "**Parties.**"

1. DEFINITIONS

For purposes of this DPA, the following capitalized terms shall have the meanings ascribed thereto. Other capitalized terms used in this DPA are defined in the context in which they are used and shall have the meanings indicated. Capitalized terms which are not defined herein shall have the meanings ascribed to them in the Agreement.

1.1 "**Adequate Country**" means: (1) for Personal Data Processed subject to the EU GDPR: (a) a member state of the EEA; or (b) a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR ("**EU Adequate Countries**"); (2) for Personal Data Processed subject to the UK GDPR: (a) the UK; or (b) a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the UK DPA ("**UK Adequate Countries**"); or (3) for Personal Data Processed subject to the Swiss FADP: (a) Switzerland; or (b) a country or territory that: (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner; or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FADP ("**Swiss Adequate Countries**").

1.2 "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et. seq.* and its implementing regulations, each as amended from time to time, including, without limitation, as amended by the California Privacy Rights Act of 2020.

1.3 "**Controller**" means the natural or legal person or entity who determines the purposes and means of the Processing of Personal Data.

1.4 "**CPA**" means the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 *et. seq.* and its implementing regulations, each as amended from time to time.

1.5 "**CTDPA**" means the Connecticut Data Privacy Act, Conn. Gen. Stat. § 45-151 *et. seq.*, as amended from time to time.

1.6 "**Customer Instructions**" means Customer's instructions to Metolius to Process Customer Personal Data on Customer's behalf: (1) as necessary to provide the Services to Customer; (2) as documented in the Agreement and this DPA; and (3) as otherwise instructed by Customer in writing and acknowledged and agreed by Metolius.

1.7 "**Customer Personal Data**" means any Personal Data Processed by Metolius on behalf of Customer via Metolius's provision of the Services. Notwithstanding anything to the contrary herein, Customer Personal Data does not include any Operational Data.

1.8 "**Data Protection Law**" means all laws, rules, regulations, and orders issued thereunder relating in any way to data protection, breach notification, privacy, or electronic marketing of any country, state, principality, or other territory that are applicable to the Processing of Customer Personal Data under the Agreement, which may include, where applicable and without limitation, CCPA, CPA, CTDPA, the European Privacy Laws, FERPA, PIPEDA, PoPIA, and/or VCDPA.

1.9 "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

1.10 "**Data Subject Request**" means a request from an individual seeking to exercise rights granted to individuals under the Data Protection Laws.

1.11 "**Europe**" means, for the purposes of this DPA, the European Union, the European Economic Area ("**EEA**"), and/or their respective member states; the United Kingdom; and Switzerland.

1.12 "**European Privacy Laws**" means all data protection laws and regulations applicable to Europe, each as amended from time to time, including: (1) with respect to the European Union, the EEA, and/or their respective member states: (a) 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 ("**EU GDPR**"); (b) Directive 2002/58/EC concerning the Processing of Personal Data and protection of privacy in the electronic communications sector (the "**E-Privacy Directive**"); and/or (c) applicable national implementations of the EU GDPR and the E-Privacy Directive; (2) with respect to Switzerland, the Federal Act on Data Protection of June 19, 1992 ("**Swiss FADP**"); and (3) with respect to the United Kingdom: (a) the Data Protection Act of 2018 ("**UK DPA**"); and (b) the retained EU law version of the General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Norther Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (SI 2019/419) ("**UK GDPR**").

1.13 "**FERPA**" means the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

1.14 "**Operational Data**" means any Customer Personal Data and any other data or information related to Customer's use of the Services that is aggregated and deidentified by or on behalf of Metolius in a manner that complies with any requirements under applicable law relating to the nature and effect of such aggregation and deidentification, and, in all cases, does not, as applicable, identify the source of such Customer Personal Data or other data or information, or with respect to any Customer Personal Data, any individual to whom such Customer Personal Data relates. For clarity, Operational Data includes, without limitation, aggregated and deidentified statistical and performance information and data created, derived, or otherwise generated in connection with Metolius's provision and operation, and Customer's use of the Services.

1.15 "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable Data Subject.

1.16 "**PIPEDA**" means the Canadian Information Protection and Documents Act, as amended from time to time.

1.17 "**PoPIA**" means the South African Protection of Personal Information Act, as amended from time to time.

1.18 "**Processing**" (including corollary terms) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, including, without limitation, collection, recording, organization, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.19 "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, or, as applicable, on behalf of a Processor.

1.20 "**Restricted Transfer**" means: (1) for Personal Data subject to the EU GDPR, the transfer of such Personal Data to, or making such Personal Data available for Processing in, any country, territory, or other jurisdiction that is not an EU Adequate Country (an "EU Restricted Transfer"); (2) for Personal Data subject to the UK GDPR, the transfer of such Personal Data to, or making such Personal Data available for Processing in, any country, territory, or other jurisdiction that is not a UK Adequate Country (a "UK Restricted Transfer"); and/or (3) for Personal Data subject to the Swiss FADP, the transfer of such Personal Data to, or making such Personal Data available for Processing in, any country, territory, or other jurisdiction that is not a Swiss Adequate Country (a "Swiss Restricted Transfer").

1.21 "**Security Breach**" means a breach of Metolius's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data on systems managed or otherwise controlled by Metolius.

1.22 "**Security Documentation**" means the security documents applicable to the specific Services provided to Customer, as updated from time to time and as made reasonably available to Customer by Metolius.

1.23 "**Services**" means those services provided by Metolius to Customer pursuant to an Agreement where, in the performance of such services, Metolius Processes Customer Personal Data on behalf of Customer as a Processor.

1.24 "**Standard Contractual Clauses**" means, generally or as context otherwise dictates: (1) where the EU GDPR or the Swiss FADP applies, the contractual clauses annexed to the Commission's implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (2) where the UK GDPR applies, the "UK Addendum to EU Standard Contractual Clauses" issued by the Information Commissioner's Office under the UK DPA ("**UK Addendum**").

1.25 "**Sub-Processor**" means a Processor engaged by Metolius to Process Customer Personal Data on Customer's behalf under the Agreement and this DPA. Sub-Processors may include third parties or Metolius's Affiliates but will not include any Metolius employee or consultant. For clarity, any independent Processor to whom Customer instructs Metolius to provide Customer Personal Data shall not be considered a Sub-Processor under this DPA.

1.26 "**Supervisory Authority**" means any applicable federal, state, or local government within the United States, or any departmental or other political subdivision thereof, or any entity, body, or authority within the United States having or asserting executive, legislative, judicial, regulatory, administrative, or other governmental functions of any court, department, commission, board, bureau, agency, or instrumentality of any of the foregoing, responsible for or involved in the enforcement and/or oversight of the Data Protection Laws.

1.27 "**VCDPA**" means the Virginia Consumer Data Protection Act, Va. Code § 59.1-575 *et. seq.*, as amended from time to time.

2. SCOPE OF DPA

2.1 **Role of the Parties.** As between Metolius and Customer, Customer shall be the Controller and Metolius shall be the Processor with respect to Customer Personal Data Processed by Metolius on Customer's behalf in connection with Metolius's provision of the Services and the Customer Instructions.

2.2 **Purpose of Processing.** The specific business purpose for which Metolius Processes Customer Personal Data on Customer's behalf pursuant to the Agreement and this DPA is to enable Metolius's provision and operation, and Customer's use, of the Services during the term of the Agreement. Customer's disclosure of Customer Personal Data to Metolius is only for the limited and specified business purpose(s) set forth in the Agreement and this DPA.

2.3 **Limitation of Obligations.** Notwithstanding anything to the contrary in the Agreement or this DPA, Customer acknowledges and agrees that Metolius has no obligation to assess Customer Personal Data in order to identify information subject to any legal requirements. Customer further acknowledges and agrees that this DPA, and Metolius's actions under this DPA, do not, and shall not be interpreted to, relieve Customer of its obligations under the Data Protection Laws and Customer shall be solely responsible for its compliance therewith.

2.4 **Operational Data.** Notwithstanding anything to the contrary in the Agreement or this DPA, Customer acknowledges and agrees that Metolius is permitted, subject to compliance with applicable Data Protection Laws, to create, collect, generate, or otherwise obtain Operational Data through or in connection with Metolius's provision and operation, and Customer's use, of the Services. Customer further acknowledges and agrees that Customer shall not acquire any right, title, or interest in or to any Operational Data.

3. CUSTOMER OBLIGATIONS

3.1 **Compliance.** Customer shall comply with the Agreement, this DPA, and the Data Protection Laws in connection with the Processing of Personal Data applicable to Customer as a Controller, including, without limitation:

(a) providing legally-compliant privacy notices to, and obtaining all necessary consents and permissions from, Data Subjects with respect to the Processing of such Data Subjects' Personal Data included within the Customer Personal Data;

(b) responding to and fulfilling Data Subject Requests in accordance with applicable Data Protection Laws; and

(c) ensuring Customer has the right to disclose to Metolius, or provide Metolius with access to, Customer Personal Data for the purpose of Metolius Processing the Customer Personal Data on Customer's behalf as contemplated under the Agreement, this DPA, and the Customer Instructions.

3.2 Accuracy and Quality of Customer Personal Data. Customer shall have the sole responsibility for the accuracy and quality of the Customer Personal Data provided by Customer to Metolius for Processing through or in connection with the Services and complying with all applicable laws, including, without limitation, the Data Protection Laws, with respect to the means by which Customer acquired such Customer Personal Data.

3.3 Customer Instructions. Customer shall be solely responsible for ensuring that all Customer Instructions comply with all applicable laws, including, without limitation, the Data Protection Laws.

3.4 Data Localization Requirements. Without limiting anything set forth in the Agreement or this DPA, Customer shall notify Metolius of any data localization requirement or restriction on the transfer of Customer Personal Data to the extent that such requirement or restriction may affect Metolius's Processing of such Customer Personal Data in accordance with the Agreement, this DPA, or the Customer Instructions.

4. METOLIUS OBLIGATIONS

4.1 Compliance.

(a) Metolius shall comply with the Agreement, this DPA, the Customer Instructions and the applicable provisions of the Data Protection Laws.

(b) Metolius shall only Process Customer Personal Data as specified in the Agreement, this DPA and the Customer Instructions or as otherwise permitted under applicable Data Protection Laws. In the event applicable law to which Metolius is subject requires Metolius to undertake other Processing of Customer Personal Data, Metolius will notify Customer (unless otherwise prohibited by such applicable law) before undertaking such other Processing.

4.2 Restrictions. Without limiting anything set forth in the Agreement or this DPA, Metolius shall not:

(a) sell or share (as and to the extent such terms are defined in the Data Protection Laws) Customer Personal Data;

(b) retain, use, or disclose Customer Personal Data for any purpose other than the business purposes specified in the Agreement or this DPA, including, retaining, using, or disclosing Customer Personal Data for a commercial purpose other than the applicable business purposes or as otherwise permitted under the Data Protection Laws;

(c) retain, use, or disclose Customer Personal Data outside of the direct relationship between Metolius and Customer except as necessary to perform the Services under the Agreement or otherwise pursuant to the Customer Instructions; and/or

(d) combine the Customer Personal Data Metolius receives from or on behalf of Customer with Personal Data Metolius receives from or on behalf of any third party or collects through Metolius's own interactions with Data Subjects, provided that Metolius may combine Customer Personal Data with other Personal Data to perform any business purpose as defined or permitted under the Data Protection Laws where applicable.

4.3 Certification. Metolius certifies to Customer that Metolius:

(a) understands and will comply with the foregoing restrictions placed on Metolius's Processing of Customer Personal Data, including complying with applicable obligations under the Data Protection Laws;

(b) will provide the same level of privacy protection as the Data Protection Laws require; and

(c) will notify Customer without undue delay if Metolius is or is likely to become unable to substantially comply with any of Metolius's material obligations under this DPA or applicable Data Protection Laws.

5. RIGHTS OF DATA SUBJECTS

5.1 Notification of Requests. In the event Metolius receives a Data Subject Request in relation to Customer Personal Data and the request identifies Customer as the Controller, to the extent reasonably possible, Metolius will, subject to compliance with applicable Data Protection Laws, at its option and in its discretion, advise the Data Subject to submit their request to Customer or notify Customer of such Data Subject Request. Customer will be responsible for responding to and fulfilling any Data Subject Request.

5.2 Metolius's Assistance. Taking into account the nature of the Processing of Customer Personal Data undertaken by Metolius, Metolius will provide reasonable assistance to Customer, through Metolius's appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of Customer's obligations to respond to a Data Subject Request under the Data Protection Laws as a Controller.

5.3 Data Subject Requests Seeking Deletion. Except as otherwise provided in the Agreement or this DPA, Metolius will promptly delete, or subject to Metolius's compliance with applicable Data Protection Laws, aggregate, anonymize or de-identify Customer Personal Data upon Customer's request in connection with an applicable Data Subject Request, unless applicable law, including, without limitation, any applicable Data Protection Laws, requires Metolius to retain such Customer Personal Data.

6. DISCLOSURES OF CUSTOMER PERSONAL DATA BY METOLIUS

6.1 Metolius Personnel. Metolius shall take reasonable steps to ensure the reliability and confidentiality of any employee, agent, or contractor who Metolius provides access to Customer Personal Data, ensuring that access is strictly limited to those individuals who need to access the

relevant Customer Personal Data for the purposes of providing the Services and as otherwise necessary to comply with Metolius's obligations under the Agreement, this DPA, the Customer Instructions, and applicable laws.

6.2 **Third Parties.** Metolius may disclose Customer Personal Data to third parties: (1) as permitted under the Agreement, this DPA, and in accordance with Customer Instructions or as otherwise necessary to perform the Services; (2) to the extent required by applicable law (subject to compliance with the Data Protection Laws); (3) to a Supervisory Authority and/or as otherwise required by the Data Protection Laws; and (4) on a "need-to-know" basis under an obligation of confidentiality or professional secrecy to its legal counsel(s), data protection advisor(s), and accountant(s).

7. SUB-PROCESSORS

7.1 **Consent to Sub-Processor Engagement.** Customer specifically authorizes Metolius to engage as Sub-Processors: (1) those entities listed in Schedule 1, attached hereto and incorporated herein by reference; and (2) all Metolius Affiliates. Without prejudice to Section 7.4 below, Customer generally authorizes Metolius to engage any other third party as a Sub-Processor at any time during the term of this DPA ("**New Third Party Sub-Processor**").

7.2 **Sub-Processor Information.** To the extent required under the Data Protection Laws, Metolius will make available to Customer information about Sub-Processors engaged by Metolius, including their respective functions and locations.

7.3 **Sub-Processor Engagement Requirements.** In connection with its engagement of any Sub-Processor, Metolius will:

(a) ensure via written contract that the Sub-Processor only accesses and uses Customer Personal Data to the extent required to perform the obligations assigned to it, and does so in accordance with a binding written agreement that imposes the same or greater obligations as Metolius's obligations set forth in this DPA; and

(b) remain fully liable for all obligations assigned to, and all acts and omissions of, the Sub-Processor in connection with such Sub-Processor's Processing of Customer Personal Data.

7.4 **Right to Object to Sub-Processor Changes.**

(a) In the event Metolius engages any New Third Party Sub-Processor during the term of an applicable Agreement, Metolius will, at least thirty (30) days before the New Third Party Sub-Processor starts Processing any Customer Personal Data, notify Customer of the engagement (including the name and location of the relevant New Third Party Sub-Processor and the activities it will perform).

(b) Customer may, within fifteen (15) days after being notified of the engagement of a New Third Party Sub-Processor, reasonably object to such New Third Party Sub-Processor. In the event Customer reasonably objects to such New Third Party Sub-Processor, Metolius will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's use of the Services to avoid Processing of Customer Personal Data by the objected-to New Third Party Sub-Processor without

unreasonably burdening Customer. If Metolius is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as its sole remedy, terminate the Agreement and this DPA by providing written notice to Metolius provided that all undisputed amounts due under the Agreement before the termination date shall be duly paid to Metolius. Until a decision is made regarding the objected-to New Third Party Sub-Processor, Metolius may temporarily suspend the Processing of the affected Customer Personal Data. Customer will have no further claims against Metolius due to Services performed by Metolius or Sub-Processors before the date of objection.

8. SECURITY AND ADDITIONAL ASSISTANCE

8.1 Security Measures. Taking into account the nature of the Processing of Customer Personal Data undertaken by Metolius for or on behalf of Customer, Metolius shall, in relation to its Processing of Customer Personal Data, implement and maintain appropriate technical, physical, and organizational measures as described in the Security Documentation, provided that such measures shall provide appropriate protections for Customer Personal Data and include appropriate and commercially reasonable technical and organizational security controls designed to prevent reasonably foreseeable accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access to Customer Personal Data in Metolius's possession or otherwise under Metolius's reasonable control and other security controls required under the Data Protection Laws (the "**Security Measures**").

8.2 Review of Security Documentation. Upon Customer's written request at reasonable intervals, but no more frequently than annually, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Metolius will make available to Customer a copy of applicable Security Documentation, which may include, based on the Services provided under the Agreement, Metolius's most recent third party audits or certifications; provided, however, that such Security Documentation shall only be used by Customer to assess Metolius's compliance with this DPA and/or the Data Protection Laws, and Customer shall not use such Security Documentation for any other purpose or disclose such Security Documentation to any third party without Metolius's prior written approval and, upon Metolius's request, Customer shall return to Metolius all such Security Documentation in Customer's possession or under its control.

8.3 Audits.

(a) Solely to the extent required under the Data Protection Laws and subject to this Section 8.3, Metolius will allow Customer, no more frequently than annually, to conduct audits (including inspections) to verify Metolius's compliance with Metolius's obligations under this DPA and/or the Data Protection Laws ("**Customer Audit**"); provided, however, any such Customer Audit, including, without limitation, any observations, conclusions, or other results of any such Customer Audit and any documents reflecting the foregoing (collectively, "**Customer Audit Results**"), shall only be used by Customer to assess Metolius's compliance with this DPA and/or the Data Protection Laws, and shall not be used for any other purpose or disclosed to any third party without Metolius's prior written approval and, subject to express requirements under the Data Protection Laws to the contrary, upon Metolius's request, Customer shall return to Metolius all such Customer Audit Results in Customer's possession or under its control.

(b) Customer must send any requests to conduct a Customer Audit of Metolius to support@metoliusgolf.com. Following Metolius's receipt of such request, Metolius and Customer will discuss and agree in advance on the reasonable start date and duration of such Customer Audit and the scope of Metolius's technical and organizational measures in scope for such Customer Audit. Notwithstanding the foregoing, unless otherwise agreed by Metolius in writing, any Customer Audit: (1) involving inspection of Metolius's business offices or data centers shall be limited to such business offices or data centers where Metolius Processes Customer Personal Data for or on behalf of Customer and shall expressly exclude inspection of or access to any premises and systems containing Personal Data Metolius Processes for or on behalf of itself or any third party that is logically but not physically separated from Customer Personal Data; (2) shall only occur during Metolius's normal business hours; (3) shall be conducted in a manner that minimizes any disruptions to Metolius's business operations; (4) shall be completed in one business day; and (5) shall be subject to all confidentiality obligations set forth in the Agreement and this DPA and Security Measures in effect at the applicable business office or data center. For the avoidance of doubt, Customer shall not have access to any information, including, without limitation, any Personal Data, of or relating to any other Metolius customer or client.

(c) Except as otherwise expressly prohibited under the Data Protection Laws, Metolius may charge a fee (based on Metolius's reasonable costs) for any Customer Audit conducted pursuant to this Section 8.3. Upon Customer's written request, Metolius will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of the applicable Customer Audit. Without limiting the foregoing, Customer will be responsible for any fees charged by any auditor appointed by Customer to conduct any such Customer Audit.

(d) Metolius may object in writing to any auditor appointed by Customer to conduct any Customer Audit if the auditor is, in Metolius's reasonable opinion, not suitably qualified or independent, a competitor of Metolius, or otherwise manifestly unsuitable. Any such objection by Metolius will require Customer to appoint another auditor or conduct the Customer Audit itself.

(e) Without limiting the foregoing, prior to conducting any Customer Audit, Customer shall undertake reasonable efforts to conduct any such Customer Audit through a review of the Security Documentation in accordance with the procedures described in Section 8.2.

8.4 Additional Reviews Under CCPA.

(a) Solely to the extent required under the CCPA and solely with respect to Metolius's Processing of Customer Personal Data subject to the CCPA ("**CCPA Data**"):

(1) Metolius grants Customer the right, upon 14 days' prior written notice, to: (1) take reasonable and appropriate steps to help ensure that Metolius uses CCPA Data Metolius receives from the Customer in a manner consistent with Customer's obligations under the CCPA; and (2) take reasonable and appropriate steps to stop and remediate Metolius's unauthorized use of Customer Personal Data; and

(2) subject to Metolius's agreement, in Metolius's sole and absolute discretion, no more frequently than annually, Customer may monitor Metolius's compliance with this DPA with

respect to Metolius's Processing of CCPA Data through additional measures that may include, ongoing manual reviews, automated scans or other technical and operational testing.

(b) For clarity, except where prohibited under the CCPA:

(1) The rights set forth in Section 8.4(a) shall be subject to any applicable limitations or requirements set forth in the Agreement or this DPA, including, without limitation, all confidentiality obligations set forth in the Agreement and exceptions to Metolius's obligations to provide the Services in accordance with any service level agreement or other service level commitment; and

(2) under no circumstances shall Section 8.4(a)(2) prohibit or otherwise preclude Metolius from: (1) declining to agree to permit Customer to perform any particular additional measures; or (2) conditioning Metolius's agreement to permit Customer to perform any particular additional measure on Customer's agreement to comply with any restrictions or requirements specified by Metolius.

8.5 **Security Breach.** In the event of a Security Breach, Metolius will notify Customer promptly and without undue delay after Metolius discovers such Security Breach. Such notification of a Security Breach will be delivered to the notice address for Customer provided in the Agreement, or, at Metolius's discretion, by telephone or other direct communication. Metolius will provide reasonable assistance to Customer to investigate, remediate, and mitigate the effects of a Security Breach and to comply with any requirements to notify affected Data Subjects, applicable Supervisory Authorities, or other third parties, all as and to the extent required under the Data Protection Laws.

9. RESTRICTED TRANSFERS

9.1 **EU Restricted Transfers and Swiss Restricted Transfers.** For any transfer of Customer Personal Data that is an EU Restricted Transfer or a Swiss Restricted Transfer, the Parties agree that such transfer shall be subject to the EU SCCs, completed as follows:

(a) the appropriate Module will apply based on the nature of the transfer, including, without limitation, the nature and role of the data exporter and data importer;

(b) in Clause 7, the optional docking clause will apply;

(c) for EU SCCs utilizing Modules Two or Three, in Clause 9(a), Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set forth in Section 7.4 of this DPA;

(d) in Clause 11(a), the optional language shall not apply;

(e) for EU SCCs utilizing Modules Two or Three:

(1) in Clause 17, Option 1 will apply and the governing laws shall be the laws of EEA member state where Customer's main business operations are located, or if no such business operations are located in any EEA member state, the Republic of Ireland; and

(2) in Clause 18(b), disputes shall be resolved before the courts of the EEA member state where Customer's main business operations are located, or if no such business operations are located in any EEA member state, the Republic of Ireland.

(f) for EU SCCs utilizing Module Four:

(1) in Clause 17, the EU SCCs shall be governed by the laws of the United States of America; and

(2) in Clause 18(b), disputes shall be resolved before the United States District Court for the District of Colorado or, in the event such jurisdiction is not available, any of the appropriate courts of the State of Colorado;

(g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I of Schedule 2, attached hereto and incorporated by reference;

(h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II of Schedule 2, attached hereto and incorporated by reference; and

(i) for EU SCCs utilizing Modules Two or Three, Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule 1.

9.2 UK Restricted Transfers. When a transfer of Customer Personal Data is a UK Restricted Transfer, the Parties agree to rely on the EU SCCs for such UK Restricted Transfers, subject to completion of the UK Addendum as follows:

(a) the EU SCCs, completed as set out in Section 9.1 shall also apply to such UK Transfers, subject to Section 9.2(b); and

(b) the UK Addendum shall be deemed completed with the information set out in Schedule 3, attached hereto and incorporated herein by reference, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of such UK Restricted Transfers.

10. RETENTION AND DESTRUCTION OF CUSTOMER PERSONAL DATA

10.1 Return and Destruction During DPA Term. Without limitation, upon Customer's request, the cessation of Metolius's provision of the applicable portion of the Services under the Agreement involving the Processing of Customer Personal Data, or the expiration or earlier termination of the Agreement, Metolius shall promptly, and in any event, within 60 days , delete, and procure for the deletion, of the applicable Customer Personal Data; provided, however, the foregoing shall not apply if and to the extent Metolius is required to retain such Customer Personal Data pursuant to Metolius's obligations under applicable laws. Notwithstanding the foregoing, Customer acknowledges and agrees that Metolius will securely erase or destroy any Customer Personal Data stored on Metolius's backup or archive systems within 90 days after Metolius's receipt of the applicable Customer Instructions.

10.2 Retention of Customer Personal Data. Notwithstanding anything to the contrary in the Agreement or this DPA and without limiting any rights provided to Metolius under the Agreement, this DPA, or applicable Data Protection Laws, to the extent authorized or required by applicable law, Metolius

may retain one copy of Customer Personal Data solely for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

11. ADDITIONAL TERMS

11.1 Liability and Indemnification. With respect to any claim, loss, or liability based upon, arising out of, resulting from, or in any way connected with a Party's performance or breach of this DPA: (1) such Party shall only be obligated to indemnify, defend, and hold the other Party harmless to the extent such obligation exists pursuant to such Party's indemnification, defense, and hold harmless obligations set forth in the Agreement (if any); and (2) each Party's total liability to the other Party is limited in accordance with the applicable limitations of liability set forth in the Agreement.

11.2 Term. This DPA shall be effective as of the DPA Effective Date and continue in full force and effect until Metolius ceases providing all Services to Customer under and in accordance with the Agreement. The provisions of this DPA which by their nature are intended to survive the expiration or earlier termination of this DPA shall continue as valid and enforceable obligations of the Parties notwithstanding any such termination or expiration. Without limitation, the provisions regarding confidentiality, compliance with applicable laws, and restrictions on the processing of Customer Personal Data shall survive the expiration or earlier termination of this DPA.

11.3 Relationship to Agreement. This DPA shall be governed by and construed in accordance with the terms set forth in the Agreement as if fully set forth herein. Without limiting anything set forth herein, the Parties acknowledge and agree that they have taken all actions (if any) required under the Agreement to incorporate this DPA therein. Any dispute arising out of this DPA shall be resolved as set out in the Agreement. The requirements set forth in this DPA are in addition to, and not in lieu of, any similar requirements set forth in the Agreement. Notwithstanding anything to the contrary in the Agreement, to the extent any conflict or inconsistency between the terms of this DPA and any Agreement, this DPA shall control. Except as set forth in this DPA, each and every Agreement remains in full force and effect, as amended, and are hereby ratified and confirmed in all respects.

11.4 Invalidity. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either: (1) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as completely as possible; or (2) if (1) is not possible, construed in a manner as if the invalid or unenforceable part had never been contained in this DPA.

11.5 Amendments. Metolius may update or modify this DPA from time to time by, without limitation, posting a revised version of this DPA on Metolius's website and publishing a general notice of such changes via the Metolius website or, as applicable and feasible, through the Services. Subject to compliance with applicable laws, Customer's access to or use of the Services after receiving notice of changes to this DPA, whether by general notice or direct notice provided by Metolius to Customer, shall constitute Customer's acceptance of such updates or modifications.

11.6 Changes to Data Protection Laws. Metolius and Customer acknowledge that the Data Protection Laws as of the DPA Effective Date may change during the term of the Agreement. Metolius and

Customer shall comply with any and all such changes to the extent applicable to the Processing of Customer Personal Data under the Agreement and this DPA.

SCHEDULE 1

METOLIUS SUB-PROCESSORS

Infrastructure Sub-Processors – Personal Data Storage and Processing

Metolius uses third party Sub-Processors to provide infrastructure services, host, and Process Customer Personal Data submitted through the Services and to help Metolius to provide customer support and email notifications. Currently, the Metolius production systems used for hosting Customer Personal Data are in co-location facilities in the United States. The following table describes the legal entities Metolius has engaged as Sub-Processors to Process Customer Personal Data together with a description of the Processing undertaken by such Sub-Processors and the countries in which they Process Customer Personal Data.

SUB-PROCESSOR	DESCRIPTION OF THE SERVICE THE SUB-PROCESSOR IS PROVIDING	SERVER LOCATION
Google Cloud Platform	**Technical infrastructure – servers, databases, web hosting, and virtual CPUs which host and/or process data.**	**United States (multi-location)** **Salt Lake City, United States**
Rocket Jones	**Software Development**	**United States (multi-location)** **Salt Lake City, United States**
Supermetrics	**Data collection and aggregation**	**EU**

Contractual Safeguards

Metolius generally requires its Sub-Processors to satisfy equivalent obligations as those imposed on Metolius under the DPA, including, but not limited to, the requirements to:

- Process Customer Personal Data in accordance with Customer's documented instructions as communicated to the relevant Sub-Processor by Metolius;
- In connection with their Processing activities undertaken as a Sub-Processor, only use personnel who are reliable and subject to a contractually binding obligation to observe data privacy and security, to the extent applicable, pursuant to applicable Data Protection Laws;
- Provide regular training in security and data protection to personnel to whom they grant access to Customer Personal Data;
- Implement and maintain appropriate technical and organizational measures (including measures consistent with those to which Metolius is contractually committed to adhere insofar as they are equally relevant to the Sub-Processor's Processing of Customer Personal Data) and provide an

annual certification that evidences compliance with this obligation. In the absence of such certification Metolius reserves the right to audit the Sub-Processor;

- Promptly inform Metolius about any actual or potential Security Breach; and
- Cooperate with Metolius in order to deal with requests from data controllers, data subjects or data protection authorities, as applicable.

The foregoing does not provide Customer any additional rights or remedies and should not be construed as a binding agreement. The information herein is only provided to illustrate Metolius's engagement process for Sub-Processors as well as to provide the actual list of Sub-Processors engaged by Metolius as Sub-Processors as of the DPA Effective Date which Metolius may use in the delivery and support of the Services.

SCHEDULE 2

ANNEX I – Details of the Processing

A. LIST OF PARTIES

Data exporter(s):

Name: Customer

Address: As specified in the Agreement.

Contact person's name, position and contact details: As specified in the Agreement

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Signature and date: The parties agree that execution of the Agreement and acceptance of the DPA by Customer shall constitute execution of these Clauses by both parties.

Role (controller/processor): Controller

Data importer(s):

Name: Metolius LLC.

Address: 2601 S. Lemay Ave #7203, Fort Collins, CO 80525

Contact person's name, position and contact detail: Ross Liggett, Managing Partner. Ross.liggett@metoliusgolf.com

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Signature and date: The parties agree that execution of the Agreement and acceptance of the DPA by Customer shall constitute execution of these Clauses by both parties.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customers or prospective customers – information about those that use a company's services, have inquired about their services, or have engaged with the company through digital technology.
- Employees – information collected about members of staff within an organization.

……..

Categories of personal data transferred

- Basic personal identifiers - information, such as name, email address, or address, that can identify an individual. This does not include information that is of a more sensitive nature.
- Identification data – information that is used to identify an individual. This may not be a name, but could also be a customer number or username that can be combined with other information to uniquely identify a person.
- Transaction & Reservation details – a record of transactions, reservations or other engagements completed by customer at the data controller's business or via their digital marketing platforms. We do not collect or transfer any payment card information.

Data transfer details

- Data is transferred continuously for the duration of the Agreement.
- Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and the DPA.
- Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and the DPA.
- The data importer will retain transferred Customer Personal Data until its deletion in accordance with the provisions of the Agreement and the DPA (as applicable).
- The subject matter, nature and duration of the Processing shall be as specified in the Agreement and the DPA (as applicable).

C. COMPETENT SUPERVISORY AUTHORITY

With respect to the EU SCCs, the data exporter's competent supervisory authority will be determined in accordance with the EU GDPR.

With respect to the UK SCCs, the data exporter's competent supervisory authority is the United Kingdom Information Commissioner's Office.

SCHEDULE 2

ANNEX II – Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Data importer shall comply with the measures set out in Metolius's Security Measures in force from time to time, including those set forth in Metolius's Security Statement, a current copy of which is located at: MetoliusGolf.com/security-statement

SCHEDULE 3

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This 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

See Annex 1.A of Schedule 2

Table 2: Selected SCCs, Modules and Selected Clauses

See Section 9 of the DPA

Table 3: Appendix Information

See Annexes I and II of Schedule 2

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in

Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.