DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is supplemental to and is incorporated by reference into the Master Service Agreement (the "**Agreement**") between Emburse and Client. The purpose of this DPA is to establish the legal basis for the processing of Client Personal Data by Emburse and, if applicable, for certain transfers of Personal Data from Client to Emburse. Unless otherwise set forth below, capitalized terms not in this DPA shall have the meaning set out in the Agreement. In the event of a conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of the DPA shall prevail.

1. INTERPRETATION

"Alternative Transfer Solution" means a mechanism other than the Standard Contractual Clauses that enables the lawful transfer of Personal Data from the EEA, UK, or Switzerland to a third country in accordance with Applicable Data Protection Laws.

"**Applicable Data Protection Laws**" means laws relating to or impacting privacy, security and the Processing of Personal Data that are applicable to the provision of Services pursuant to the Agreement, including CCPA and GDPR.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., and any amendments or implementing regulations thereto, including the California Privacy Rights Act of 2020 (CPRA), that are or become effective on or after the effective date of this DPA.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. In the context of CCPA it shall have the meaning given to "business" in CCPA.

"**Data Subject**" means an identified or identifiable natural person. In the context of GDPR and UK GDPR "Data Subject" shall have the meaning given to such term in GDPR and UK GDPR and in the context of CCPA it shall have the meaning given to "consumer" in CCPA.

"**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and any national Law of the European Economic Area member states ("**EEA**") implementing or supplementing this regulation, in each case as amended, replaced or superseded from time to time, and all applicable Laws of the European Union or the EEA member states with regard to the Processing of Personal Data.

"**Personal Data**" means information pertaining to individuals that is referred to as "personal data", "personally identifiable information", "personal information", "personal health information" or other reasonably equivalent terms within the scope of Applicable Data Protection Laws

"**Processing**" means any operation or set of operations that is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, and "**Process**" and "**Processes**" will be interpreted accordingly.

"**Processor**" means, as applicable, (a) the entity that Processes Personal Data on behalf of a Controller, (b) the "service provider" as such term is defined in the CCPA, and (c) any person or entity within the scope of another reasonably equivalent term under another Applicable Data Protection Law.

"**Services**" means the services provided by Emburse to Client under the Agreement.

"Standard Contractual Clauses" or "**SCC**" means (i) with respect to the GDPR, "Module Two: Transfer controller to processor" of the Standard Contractual Clauses of June 4, 2021 posted here[1] (or on any successor URL or Web page); (ii) with respect to UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum"), in force March 21 2022 posted here[2] (or on any successor URL or Web page); and (iii) with respect to data exclusively subject to the FADP, has the same meaning as the GDPR SCC with the exception of the adaptations set out in Section 5.2(d) of this DPA.

"**UK GDPR**" means data privacy laws in the United Kingdom that correspond to GDPR.

"**FADP**" means the Swiss Federal Act on Data Protection of June 19, 1992 and its revised version of September 25, 2020.

2. ROLES OF THE PARTIES

2.1 Controller and Processor.

(a) For purposes of the GDPR and UK GDPR and any and all other Applicable Data Protection Laws, Client and its Affiliate(s), as applicable, is the Controller of Client Personal Data, and Emburse is the Processor of such data. Emburse shall ascertain and comply with its obligations as a Processor under Applicable Data Protection Laws, and shall immediately notify Client if it makes a determination that it can no longer fulfil such obligations.

(b) For purposes of the CCPA, Client or Client's Affiliate(s), as applicable, is the "business" (as defined in Cal. Civ. Code §1798.140), and Emburse will act as a "service provider" *(ibid.)* in its performance of its obligations under the Agreement. Emburse will not retain, use, or disclose any "personal information" *(ibid.)* included in the Client Personal Data for any purpose other than Emburse's performance of its obligations under the Agreement, or as otherwise permitted by the CCPA. Emburse will not "Sell" or "Share" (as defined in the CCPA/CPRA) any Personal Data to another business or third party without the prior written consent of Client, nor combine Personal Data Emburse receives from, or on behalf of, Client with Personal Data received from other sources.

2.2 Client Affiliates. If Personal Data of Client's Affiliate(s) is Processed, Client's Affiliate(s) providing such data shall have the same rights as the Client under this DPA. Except where applicable Data Protection Laws require Client's Affiliate to exercise a right or seek any remedy under this DPA against Emburse directly, the Parties agree that: (i) Client shall exercise any such right or seek any such remedy on behalf of the Affiliate, and (ii) Client shall exercise any such rights under this

[1] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914

[2] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

DPA not separately for each Affiliate but in a combined manner for itself and all of its Affiliates together.

3. SPECIFICATION OF THE DATA PROCESSING

3.1 Instructions for Data Processing. Emburse will only Process Client Personal Data in accordance with the Agreement, to the extent necessary to provide the Services to Client and fulfil Client's instructions, provided in electronic or written form (referred to collectively as "in writing") or, if provided verbally, confirmed in writing.

3.2 Scope of Processing. Processing outside the scope of this DPA or the Agreement will require prior written agreement between Client and Emburse on additional instructions for Processing. Should Emburse reasonably believe that a specific Processing activity beyond the scope of Client's instructions is required to comply with a legal obligation that Emburse is subject to, Emburse shall inform Client and seek explicit authorization from Client before undertaking such Processing. Emburse shall never process the Personal Data in a manner inconsistent with Client instructions. Emburse shall promptly notify Client, if, in its opinion, any instruction violates Applicable Data Protection Law.

3.3 Scope, Purpose and Duration of the Processing. The scope and purpose of the processing, as well as the types of personal data and categories of data subjects concerned are set out in Schedule A of this DPA (notwithstanding the inclusion of same or similar details or information in the Order Form or in a SOW). The duration of the Processing and this DPA coincides with the duration of the applicable Order Form or SOW.

4. SUBPROCESSORS

4.1 Authorized Subprocessors. Emburse shall not permit subprocessors to Process Client Personal Data except as authorized in this DPA. Client authorises Emburse to engage the subprocessors listed here for the Processing activities set forth in Schedule A. Emburse shall inform Client in writing thirty (30) days in advance of any addition or replacement of such subprocessor giving Client an opportunity to object to such changes. If Client timely sends a written notice, setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve Client's objection. In the absence of a resolution, Emburse will make commercially reasonable efforts to provide Client with the same level of Services set out in the Agreement, without using the subprocessor. If Emburse's efforts are not successful within a reasonable time, each Party may terminate the portion of the Service which cannot be provided without the subprocessor, and Client will be entitled to a pro-rated refund of the applicable Service Fees.

4.2 Obligations. Emburse shall ensure that the subprocessor is bound by a written agreement setting out data protection obligations compatible with those of Emburse under the Agreement including this DPA, shall supervise compliance thereof, and must in particular impose on its subprocessors the obligation to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of Applicable Data Protection Laws.

4.3 Liability. Notwithstanding any Client authorization for Emburse to use subprocessors, Emburse shall remain fully liable to Client for the acts and omissions of such subprocessor that fails to fulfil its data protection obligations as if they were the acts and omissions of Emburse.

4.4 Audit. Client may request that Emburse audit a subprocessor or provide confirmation that such an audit has occurred (or where available, obtain or assist Client in obtaining a third-party audit report concerning the subprocessor) to ensure compliance with its obligations imposed by Emburse in conformity with this Agreement.

5. INTERNATIONAL TRANSFERS OF PERSONAL DATA

5.1 Transfer of Data. In the case of a transfer of Personal Data to a country not ensuring an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data pursuant to Applicable Data Protection Laws, the Parties shall cooperate to ensure compliance with the Applicable Data Protection Laws, including as set out in the following Sections.

5.2 Transfer Mechanisms. Unless there is an Alternative Transfer Solution, Client Personal Data originating in the EEA, Switzerland or UK may only be exported to or accessed by Emburse or its subprocessors outside the EEA, Switzerland or UK as follows:

(a) The Client Personal Data originating in the EEA, Switzerland or UK shall be transferred in adherence to the Standard Contractual Clauses and the parties agree that their execution of the Agreement will be deemed as their respective acceptance and execution of the Standard Contractual Clauses including the warranties and undertakings contained therein.

(b) With respect to the GDPR, each to itself as applicable with respect to the transferred Personal Data agrees to select the following options under the SCC:

(i) Clause 7 – the Docking Clause shall apply.

(ii) Clause 9 – Option 2: General Written Authorisation: The data importer has the data exporter's general authorisation for the engagement of subprocessor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the subprocessor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(iii) Clause 11 – the optional language in the Clause is not used and is deleted.

(iv) Clause 17 – Option 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of Ireland.

(v) Clause 18 – Any disputes arising from these Clauses shall be resolved by the courts of Ireland.

(vi) Details required under Annex I of the SCC are available in Annex 1 to this DPA. Details required under Annex II of the SCC are available in Annex 2 to this DPA. If there is an inconsistency between any of the provisions of this Addendum and the provisions of the SCC, the provisions of the latter shall prevail.

(c) With respect to the UK GDPR, details required by Tables 1-3 under Part 1 of the UK Addendum are available in Annexes 1, 2, and 3 to this DPA, and in Section 1 of this DPA under "Standard Contractual Clauses" (for module in operation) and Section 5.(b)(i)(ii)(iii) of this DPA (for

Clauses 7, 9a, and 11 options). With respect to Table 4 in Part 1 of the UK Addendum, the UK Addendum may be ended as set out in its Section 19 by the Exporter. If there is an inconsistency between any of the provisions of this DPA and the provisions of the SCC, the provisions of the latter shall prevail.

(d) With respect to data exclusively subject to the FADP, the following adaptations apply to the SCC: (i) the competent supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC); (ii) the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c; (iii) references to the GDPR are to be understood as references to the FADP, and (iv) the SCC also protect the data of legal entities until the entry into force of the revised FADP. For the sake of clarity, no adaptations are made for SCC Clauses 17 and 18.

6. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

6.1 Emburse Confidentiality. Emburse shall treat all Persona Data as Confidential Information, adhere to the confidentiality obligations set out in the Agreement and termination or expiration of the Agreement shall not discharge Emburse from its confidentiality obligations. Emburse shall limit access to Client Personal Data to those employees or other personnel who have a business need to have access to such Client Personal Data to provide the Services. Further, Emburse employees shall be committed to protect the confidentiality and security of Client Personal Data in accordance with the provisions of this DPA and the Agreement.

6.2 Emburse Security Obligations.

(a) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Emburse shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data transmitted, stored or otherwise processed. Without limiting the generality of the foregoing, Emburse shall put in place and maintain the technical and organisational measures as set out in Schedule B of this DPA to protect Client Personal Data against any Security Incident. If the Client Personal Data will include any payment card information, Emburse shall comply with all applicable requirements of the Payment Card Industry Data Security Standard.

(b) Emburse shall maintain written information security policies that are fully applicable to the Processing of Client Personal Data and appropriate to the risks of the Processing. Such policies shall include the technical and organization measures set out in Schedule B.

6.3 Client Security Obligations. Client agrees that, without limiting Emburse's obligations under Section 6.2, Client is responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of Client Personal Data, including complying with Emburse acceptable use or other policies; (b) securing the account authentication credentials, systems and devices Client uses to access the Services; (c) securing Client's systems and devices that Emburse uses to provide the Services; (d) backing up Client Personal Data; (e) obtaining any required consents from Data Subjects for the Processing of Client Personal Data; and (f) limiting the transfer to Personal Data that is strictly necessary for Emburse to provide the Services Client has contracted.

6.4 Changes in Security Measures. Emburse will evaluate the security measures implemented on an ongoing basis and may, from time to time modify the technical and organizational measures to ensure adequate protection of the Client Personal Data considering the advancement of technology and rising new threats. However, the overall security must not fall below the agreed level of security thereafter.

6.5 Emburse Self-Audit. Emburse shall implement a data protection management procedure appropriate to the risks of the Processing of Client Personal Data for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the Processing and compliance with this Agreement.

6.6 Client Security Audits. At the request of Client, Emburse shall demonstrate, including through any third-party certifications, the security measures it has taken. Should Client provide well-founded indications that such information does not reasonably demonstrate compliance with the security measures set out in this DPA (including the technical and organisational measures as set out in Schedule B of this DPA) or an audit is requested by a supervisory authority, Emburse shall allow Client to audit, by itself or using an independent third-party auditor (acceptable to Emburse and subject to a non-disclosure agreement), Emburse's compliance, including by conducting an audit of Emburse's data processing facilities. Such audits may be performed at most once annually. Client shall give Emburse no less than thirty (30) days' notice of any audit. Client and Emburse shall cooperate in good faith to agree a plan covering the scope, duration, and activities of the audit, including necessary precautions to maintain the confidentiality of Emburse data that is outside the scope of the audit. Emburse shall cooperate with such audits and shall grant Client and its auditors reasonable access to any premises, systems, and devices involved with the Processing of the Personal Data as may be reasonably required by Client to ascertain Emburse's compliance with this DPA and Applicable Data Protection Laws. The records and results of such Audit shall be deemed Emburse Confidential Information under the Agreement. Client shall bear all its own costs and expenses of audit.

6.7 Security Incident

(a) In the event Emburse discovers a personal data breach (as defined in Applicable Data Protection Laws by this or reasonably equivalent term) affecting Client Personal Data (a "**Security Incident**"), Emburse will inform Client of the Security Incident without undue delay, and no later than within seventy-two (72) hours of Emburse's discovery of such Security Incident.

(b) Emburse's Security Incident notification will contain the information necessary (insofar as such information is in the possession of or available to Emburse) to allow Client to meet its obligations under Applicable Data Protection Laws to notify supervisory authorities, data subjects, and

other required parties. Emburse's notification of or response to a Security Incident shall not be construed as acknowledgement of any fault or liability with respect to the Security Incident.

(c) Emburse will investigate and work to remediate the Security Incident and cooperate with Client (and any law enforcement or regulatory officials) in Client's handling of the matter, including any investigation, reporting or other obligations required by Applicable Data Protection Law.

(d) Notwithstanding Company's obligations under parts (a), (b), and (c) of this Section 6.7, Client is solely responsible for complying with any obligations under Applicable Data Protection Laws to notify third parties of the Security Incident. Emburse will not notify any third party of the Security Incident without Client's prior, written authorization. Further, Emburse agrees that Client will have the sole right to determine: (a) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by Applicable Data Protection Law, or otherwise in Client's discretion; and (b) the contents of such notice, whether any type of remediation may be offered to any affected third parties, and the nature and extent of any such remediation. Emburse will maintain and preserve all documents, records, and other data related to any and all Security Incidents, until directed by Client to destroy such documents. Emburse will cooperate with Client in any and all litigation, investigation, or other action deemed necessary by Client to protect its rights relating to the Security Incident.

(e) Emburse will reimburse Client and its Affiliates for any actual reasonable Security Incident Costs incurred by Client, its Affiliates or subsidiaries, arising out of or in connection with a Security Incident attributable to Emburse's noncompliance with this DPA to the extent such costs relate to activities required under Applicable Data Protection Laws.

(f) Client shall be fully responsible for any time spent by Emburse (at Emburse's then-current professional services rates) for any cooperation and assistance requested by, and provided to, Client that is over and above that required under Applicable Data Protection Laws and this Section 6.7.

7. DATA SUBJECT RIGHTS, REGULATORY INVESTIGATIONS, LITIGATION

7.1 Data Subject Requests. Emburse shall promptly notify Client if it receives a request, related to Client Personal Data, to exercise rights provided to Data Subjects in Applicable Data Protection Laws, including but not limited to requests for access, correction, or deletion. Emburse shall not respond directly to the Data Subject nor act on the request unless expressly authorized in writing by Client to do so and will provide Client with assistance to fulfil such requests as required by Applicable Data Protections Laws, including as required by adopting appropriate technical and organizational measures.

7.2 Regulatory Investigations or Litigation. Emburse shall promptly notify and provide Client with assistance in connection with any regulatory investigations or litigation related to Client Personal Data

8. ASSISTANCE

8.1 Emburse's Assistance. In addition to assistance provided under Section 7 above, and taking into account the nature of the Processing and the information available to Emburse, Emburse shall assist Client in complying with the obligations pursuant to Applicable Data Protection Laws including providing reasonable assistance with (i) any data protection impact assessments which are referred to in Article 35 of the GDPR and UK GDPR, and (ii) with any prior consultations to any applicable supervisory authorities which are referred to in Article 36 of the GDPR and UK GDPR, in each case solely in relation to Processing of Client Personal Data.

8.2 Client's Assistance. Client will reasonably assist Emburse in complying with all Applicable Data Protection Law applicable to Emburse in its performance of the Services.

8.3 Required Disclosure. Emburse shall promptly notify Client of any request for the disclosure of Client Personal Data by a governmental regulatory body, law enforcement authority, or any other applicable supervisory authority, unless otherwise prohibited by applicable law or a legally binding order of such body or agency.

9. EFFECT OF TERMINATION

9.1 Handling of Data. Without limiting the generality of any related terms in the Agreement**,** Emburse shall promptly and in any event within no later than thirty (30) days of the date of expiration or termination of the Agreement (or within such shorter timeframe as may be required by the Agreement or an applicable SOW) delete and destroy and procure the deletion and destruction of all copies of Client Personal Data held by Emburse or any subprocessors. On Client's written instruction (to be received by the date of expiration or termination of the Agreement), Emburse shall within thirty (30) days return a complete copy of Client Personal Data by secure file transfer in such common industry-standard format as notified by Client.

9.2 Retention of Data. Emburse may retain Client Personal Data to the extent required by applicable Law only to the extent and for such period as required by such applicable Law, and provided that Emburse shall ensure the confidentiality of all such Client Personal Data in accordance with this DPA and the Agreement and shall ensure that it is only Processed as necessary for the purpose(s) specified in such Laws requiring its storage and for no other purpose.

9.3 Written Certification. On Client's written request, Emburse shall provide written certification to Client that it has fully complied with the foregoing obligations promptly upon their fulfilment.

***

Schedule A – Scope of the Processing
(To be completed by the parties)

Categories of Individual

Emburse will process data about the following categories of individuals:

(A) ☒ Client employees
(B) ☐ Client business contacts (for example, contacts at customers, prospects, vendors, partners)
(C) ☐ Visitors to Client public websites
(D) ☐ End-users of Client services
(E) ☒ Other: Potentially other individuals mentioned in client employee reports uploaded to the Services

Categories of Personal Data

Emburse will process the following categories of data about the individuals:

(A) ☒ Client internal information and records
(B) ☒ Client business contacts data (sometimes called "business card information")
(C) ☐ Client public website browsing information (including device identifiers and data collected via cookies, logs, etc.)
(D) ☐ Client services end-user identifiers and contact/employment information (for example, names, emails, addresses, phones, employer)
(E) ☐ Data stored in end-user accounts
(F) ☐ Client services usage information (for example, end-user log-in times, pages visited, and content viewed, including when associated to device identifiers and collected via cookies, logs, etc.)
(G) ☐ Other: Specify _____

Sensitive Personal Data

If Emburse will not process sensitive personal data, leave blank.

(A) ☐ Gender
(B) ☐ Race/ethnicity
(C) ☐ Health Data ("PHI")
(D) ☒ Financial account numbers
(E) ☐ Other: Specify _____
[Other categories of sensitive data include: political, philosophical, and religious opinions/beliefs; trade union membership; genetic; biometric; sex life; government ID numbers.]

Brief Description of Processing Activity and Processing Activity Purpose

Example: Emburse will process the personal data in order to provide the Services set out in the Agreement.

_____

_____

Schedule B – Technical and Organizational Measures

The technical and organizational measures implemented by Emburse are set out in Emburse's **Information Security Addendum (ISA)** posted on Emburse website or on any successor web page.

Annex 1
(Parts A & B to be completed by the parties)
(Only if Standard Contractual Clauses are required per Section 5 of this DPA)

A. LIST OF THE PARTIES

Data Exporter (s): [*Identity and contact details of the data exporter(s) and, where applicable of its/their data protection officer and/or representative in the European Union*]

Exporter	
Legal Name:	
(UK SCC only) Official registration number (if any)	
Trading Name (if different)	
Address:	
Contact person's name, position and contact details:	EU Representative:
Activities relevant to the data transferred under these Clauses:	
Signature and Date	
Role	Controller

Data Importer (s): [*Identity and contact details of the data importer(s) and, where applicable of its/their data protection officer and/or representative in the European Union*]

Importer	
Legal Name:	Emburse, Inc.
(UK SCC only) Official registration number (if any)	N/A
Trading Name (if different)	N/A
Address:	TBC
Contact Person's name, position and contact details:	Bill Bowman, DPO, privacy@emburse.com
Activities relevant to the data transferred under these Clauses:	Transfers necessary for the purpose of processing data as stipulated on the Order Form
Signature and Date	
Role	Processor

B. DESCRIPTION OF THE TRANSFER

***Categories of Data Subjects whose personal data is transferred*:** List the Categories of Individual from Schedule A whose personal data will form part of the transfer (e.g. A, D, F) A, E

Categories of personal data transferred: List the Categories of Personal Data from Schedule A that will be included in the transfer (e.g. B, C, E) A, B

***Sensitive data transferred*:** If applicable, list the Sensitive Personal Data from Schedule A that will be included in the transfer (e.g. A, E) None

Applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. See details in the body of this DPA and in Schedule A and Schedule B.

The frequency of the transfer (e.g. whether the data is transferred on one-off or continuous basis): The data will be transferred on a continuous basis during the term of the Agreement.

Nature of the processing: See Schedule A.

***Purposes of the data transfer(s) and further processing*:** See Schedule A.

***The Period for which the personal data will be retained, of if that is not possible, the criteria used to determine that period*:** See Section 9 of this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the supervisory authority/ies in accordance with Clause 13: Pursuant to Clause 13

Annex 2
Technical and Organizational Measures
Including Technical and Organizational Measures to Ensure the Security of the Data
(To be completed by the parties)

The technical and organizational measures are described in Schedule B of this DPA