# DATA PROCESSING AGREEMENT
# FOR CUSTOMERS (ORDER FORM)

This Data Protection Agreement, including its Addenda ("**DPA**"), is by and between the Emburse entity and the Customer entity named in the Order Form to which this DPA is attached. This DPA is hereby incorporated into and made a part of the Terms and Conditions also attached to the Order Form (collectively the "**Agreement**"). This DPA shall supersede the Terms and Conditions but only to the extent this DPA expressly sets forth terms for Processing Personal Data and for compliance with Data Protection Laws, whenever there is a conflict between the Standard Contractual Clauses ("SCC") and this DPA, the SCCs shall control. All capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

## 1. Purpose and Scope

1.1. This DPA shall govern the Processing of Personal Data through the parties' performance of the Agreement in compliance with Data Protection Laws. The subject matter, nature, and purpose of the Processing, type of Personal Data, categories of Data Subjects, and the appropriate technical and organizational measures for security of Personal Data as set forth in Addendum I.

1.2. Emburse Sub-processors list is available at https://www.emburse.com/legal/sub-processors.

1.3. EU Standard Contractual Clauses and the UK International Data Transfer Agreement are set forth in Addenda II and III.

1.4. This DPA is intended for purposes of compliance with Data Protection Laws as defined in Section 13.

1.5. Customer shall be the Controller or Data Exporter and Emburse shall be the Processor or Data Importer as defined in Section 13.

## 2. Compliance Responsibilities

### Emburse

2.1. Emburse shall Process Personal Data in compliance with Data Protection Laws and this DPA.

2.2. Emburse shall Process Personal Data in accordance with Customer's documented instructions but only if such instructions are: (i) based in and for the purpose of performing the terms of the Agreement; (ii) in compliance with Data Protection Laws;

and (iii) do not differ from or exceed the functionality the Service. Emburse shall promptly notify Customer if, in Emburse's commercially reasonable opinion, Emburse is unable to comply with such instruction or such instruction is not in compliance as set forth in (ii) above, or Emburse is required by applicable law or order to Process the Personal Data, provided that Emburse is not prohibited by law from notifying Customer.

2.3. Emburse shall make commercially reasonable efforts to limit disclosure or access to Personal Data to any employee, agent, or contractor who need to know or have access to the Personal Data for Emburse's provision of the Service and performance of the Agreement, and direct its Sub-processors to undertake the same.

2.4. Emburse shall, to the extent permitted by applicable law, promptly notify Customer if Emburse receives a request from a Data Subject to exercise the Data Subject's rights of access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, or objection to the Processing. Emburse shall reasonably cooperate with Customer in responding to such Data Subject requests, subject to Section 2.11.

2.5. Emburse shall maintain a written record of Processing including the name and contact details of the Customer and Sub-Processors, Emburse's data protection officer or representative, categories of Processing, transfers of Personal Data, and, as practicable, a general description of appropriate safeguards. Emburse shall make such written records available to a Supervisory Authority upon Supervisory Authority's request.

**CUSTOMER**

2.6. Customer shall export, transfer, and otherwise provide Personal Data to Emburse in compliance with Data Protection Laws and this DPA.

2.7. Customer shall be solely responsible for certifying that all the conditions mentioned in Section 2.2 are met. Customer shall promptly notify Emburse if any of the aforementioned conditions are not met or if Customer cannot meet the conditions after Processing has begun.

2.8. Customer shall have sole responsibility for obtaining any and all relevant agreements, authorizations, consents, instructions or permissions for the Processing of Personal Data from Data Subjects and Customer's client(s) for Emburse to Process Personal Data on Customer's behalf.

2.9. Customer shall have sole responsibility for the accuracy, completeness, format, and legality of Personal Data.

2.10. Customer certifies that Customer will limit the transfer to Personal Data that is strictly necessary for Emburse to provide the Services Customer has contracted.

2.11. Customer shall have primary responsibility for receiving, responding to, and resolving any request, complaint or inquiry from a Data Subject, Supervisory Authority, or third party, at Customer's sole cost and expense. Emburse shall promptly notify the Customer of any request, complaint, or inquiry received directly by Emburse. Emburse shall reasonably cooperate with the Customer in the response to such request, complaint, or inquiry, to the extent Emburse is permitted or required by applicable law. If Customer seeks a protective order against such request, complaint, or inquiry, Emburse shall reasonably cooperate with Customer, to the extent permitted by applicable law.

2.12. Customer shall have primary responsibility for the investigation, notification, remediation and mitigation of a Personal Data Breach, at Customer's sole cost and expense (unless otherwise agreed in Section 10.2 of Emburse's Terms and Conditions). Emburse shall commercially reasonably cooperate with Customer in fulfilling Data Protection Law requirements regarding Personal Data Breach.

2.13. Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Emburse directly, the parties agree that: (i) Customer shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) Customer shall exercise any such rights under this DPA not separately for each Authorized Affiliate but in a combined manner for itself and all of its Authorized Affiliates together.

## 3. SECURITY

3.1. Taking into account the state of the art, the nature, scope, context, and purposes of Processing, Emburse shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including: (i) pseudonymization and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

3.2. Emburse may change the technical and organizational measures set out in Addendum I at any time without notice to Customer, provided such changes do not diminish the then current security of Personal Data provided by Emburse.

## 4. SUB-PROCESSORS

4.1. Customer hereby grants Emburse general authorization to appoint Emburse Affiliates and third parties to Process Personal Data as Sub-processors, which general authorization Emburse shall flow down to Emburse Sub-processors' vendors. A list of Emburse Sub-processors is available at

https://www.emburse.com/legal/sub-processors. Emburse may add or delete Sub-processors published on Emburse's website. Customer should visit the site periodically for updates.

4.2. Sub-Processors shall Process Personal Data for Emburse under a written contract executed by Emburse and Sub-processor that includes: (i) materially similar data protection obligations as set out in in this DPA; (ii) the implementation of appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Laws; and (iii) Standard Contractual Clauses.

4.3. Emburse shall be liable for the Processing of Personal Data by its Sub-processors to the same extent Emburse would be liable under this DPA for Processing Personal Data itself.

4.4. Customer may avail itself of all other rights regarding Sub-processors set forth in the Standard Contractual Clauses.

## 5. Personal Data Breach Notification

5.1. Emburse shall notify Customer of a confirmed Personal Data Breach affecting Customer's Personal Data, without undue delay and, where feasible, not later than seventy two (72) hours. Said notification by Emburse to Customer shall, to the extent the available to Emburse, include the following: (i) the approximate number of Data Subjects and categories of Personal Data affected by the Personal Data Breach; (ii) a point of contact for Customer to receive further information from Emburse about the Personal Data Breach; (iii) the likely consequences of the personal data breach; and (iv) the measures taken or proposed to be taken by Emburse to investigate and remediate the Personal Data Breach.

5.2. Customer shall be responsible for all Controller obligations regarding the notification of Data Subjects and Responsible Authorities of a Personal Data Breach affecting Customer's Personal Data. Such actions shall include the establishment of a point of contact for Customer's receipt and response to inquiries from Data Subjects, and an electronic method of providing information to Data Subjects regarding the Personal Data Breach.

5.3. Customer shall bear the financial responsibility under Section 5.2 (unless otherwise agreed in Section 10.2 of Emburse's Terms and Conditions).

5.4. Emburse shall, at Emburse sole cost and expense, be responsible for notifying the Supervisory Authorities of a Personal Data Breach, provided that Emburse is required to do so by law in its capacity as a Processor.

## 6. Data Protection Impact Assessment

6.1. Emburse shall provide commercially reasonable assistance to Customer to carry out, upon Customer's written request, a Data Protection Impact Assessment, but only to the extent required by Data Protection Law and to the extent the Data Protection Impact Assessment cannot be carried out by Customer without Emburse's assistance. Customer shall bear sole cost and expense for a Data Protection Impact Assessment and Customer shall reimburse Emburse for any costs and expenses incurred by Emburse in providing such assistance.

## 7. Retention and Deletion of Personal Data

7.1. Emburse, its Affiliates and Sub-processors shall retain Personal Data for the period of time required by Data Protection Laws, other applicable laws or regulations, and as needed to comply with its legal and contractual obligations.

7.2. Upon (i) ninety (90) days following the effective date of termination of the Order Form and cessation of the associated Processing of Personal Data, as applicable; or (ii) the expiration of the retention periods required by Data Protection Laws, other regulations, or legal processes, Emburse shall destroy, anonymize, or pseudonymize all copies of such Personal Data, and direct its Sub-processors to undertake the same. Emburse shall provide to Customer a certification of the destruction, anonymization or pseudonymization of Personal Data upon Customer's request.

7.3. During the term of the Agreement, Customer may access, export, and retrieve Customer Personal Data in a standard format. Export and retrieval of Personal Data may be subject to technical limitations. If export and retrieval is not technically possible, Emburse and Customer shall determine a commercially reasonable method of export and retrieval including their respective costs and expenses to the extent permitted by applicable Data Protection Laws.

7.4. Upon Customer's written request to Emburse within thirty (30) days after the effective date of termination, Emburse shall (i) permit Customer access to the Service for thirty (30) days after termination for the sole purpose of export and retrieval, or (ii) subject to applicable fees (at its then current rate Emburse chargers its customers for such effort), provided that Customer has paid all fees due under the Agreement.

## 8. Certifications and Audits

8.1. Emburse shall reasonably provide to Customer information on Emburse's technical and organizational measures as set forth in this DPA, including third party certifications and security documentation, upon the written request of Customer.

8.2. Customer may reasonably audit Emburse's Processing if: (i) Emburse fails to provide the information required under Section 8.1, or (ii) an audit is requested by a Supervisory Authority.

8.3. Customer may not request such an audit more than once in any twelve (12) month period, such limitation shall not apply in case of a Personal Data Breach. Emburse acknowledges a Supervisory Authority may require more frequent audits of Emburse's Processing.

8.4. If a Customer requests an audit, such audit shall be conducted by an independent auditor who, in Emburse's sole discretion, is not considered an Emburse competitor.

8.5. If multiple customers request an audit, Customer acknowledges and agrees that Emburse may demand that Customer's audit is combined with that of the other customers.

8.6. Customer shall give Emburse at least sixty (60) days prior written notice of any audit initiated pursuant to Section 8.2. The date, time, place, and scope of such audits shall be mutually agreed by the parties. Audits shall be limited to three (3) days. Customer shall make, and ensure that their independent auditors make reasonable efforts to avoid and mitigate risk of any damage, injury, or disruption to Emburse premises, equipment, personnel, operations, services, and business in the course of such audit.

8.7. Customer shall bear all costs and expenses of audits initiated pursuant to Section 8.3, provided that Customer reimburses Emburse for Emburse's costs and expenses to the extent said costs and expenses arise from (i) any auditing conducted in breach of this Section 8 or (ii) any auditing which is extraordinary to industry standards and best practices. Emburse shall bear reasonable costs of an audit in case of Personal Data Breach, provided that said audit is required by Data Protection Laws.

8.8. Customer acknowledges and agrees that Emburse may deny access to information that, in Emburse sole discretion, may be considered confidential and thereby protected from disclosure. However, Emburse shall, whenever possible, provide Customer with redacted versions of the requested information. Customer understands that such requests may be costly, as such Customer shall bear all costs and expenses related to the production of redacted documents.

## 9. Restricted International Data Transfers

### 9.1. EEA Restricted International Data Transfers - Standard Contractual Clauses

9.1.1. Emburse and Customer agree that in respect to Restricted International Transfers subject to GDPR the parties hereby enter Module 2 of the EEA Standard Contractual Clauses.

9.1.2. Module 2 of the EEA Standard Contractual Clauses shall also apply to Restricted International Transfers affecting Personal Data originated in Switzerland.

9.1.3. Module 2 of the EEA Standard Contractual will come into effect upon the commencement of a Restricted International Transfer.

9.1.4. Customer shall be the Data Exporter and Emburse shall be the Data Importer.

9.1.5. Customer and Emburse agree to the following:

9.1.5.1. Clause 7 - *Docking Clause* shall apply

9.1.5.2. Clause 9(a) - *Use of Sub-Processors* Option 2 shall apply and the "time period" shall be 30 days.

9.1.5.3. Clause 11(a) - *Redress* optional language shall not apply.

9.1.5.4. Clause 13(a) - *Supervision*

9.1.5.4.1. Where Customer is established in an EU Member State, the following shall apply: "*The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex 1(C), shall be the supervisor authority of the Member State in which Customer is established of (if different) the lead supervisory authority of the Customer in respect of a cross-border processing activity*;" OR

9.1.5.4.2. Where the Customer is not established in an EU Member State, but falls within the territorial scope of the application of the GDPR, in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR the following shall apply: "*The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of the Regulation (EU) 2016/679 is established, as indicated in Annex 1(C), shall act as the competent authority*;" OR

9.1.5.4.3. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative the following shall apply: "*The supervisory authority of one of the Member States in which the data subjects whose personal data in transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex 1(C), shall act as a competent supervisory authority*"

9.1.5.5. Clause 17 - *Governing Law* Option 2 shall apply and the "Member State" shall be Germany

9.1.5.6. Clause 18 - *Choice of Forum and Jurisdiction* the Member State shall be Germany

9.1.5.7. Annex 1

9.1.5.7.1. Customer shall be the Data Exporter

9.1.5.7.2. Emburse shall be the Data Processor

9.1.5.7.3. The Processing operations shall be those specified in the Agreement and supporting documents

9.1.5.8. Annex 2 - See Addendum I

9.1.5.9. Annex 3 - Not applicable

9.2. **UK Restricted International Data Transfers**

9.2.1. In cases of Restricted International Data Transfers subject to UK GDPR, the EEA Standard Contractual Clauses shall be read alongside with, and amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA.

9.2.2. Emburse and Customer agree that the information required for the completion of Part 1 of the UK IDTA shall be included in Addendum III.

9.3. **Emburse and Sub-Processors Restricted International Transfer**s

9.3.1. Emburse and its Sub-Processors shall enter Module 3 of the EEA Standard Contractual Clauses whenever appropriate and necessary for compliance with Data Protection Laws.

9.3.2. Emburse and its Sub-Processors shall enter the UK IDTA whenever appropriate and necessary for compliance with Data Protection Laws.

9.4. **Amendments, Updates, Additional Protections**

9.4.1. Emburse and Customer acknowledge and agree that if the European Commission and/or the UK Government issue any amendment or replacements of the Standard Contractual Clauses pursuant to Article 46(5) of the GDPR or Article 46 of the UK GDPR, such clauses will automatically become in full force and effect.

9.4.2. Emburse and Customer agree that if at any time during the length of the Agreement a Supervisory Authority or court of competent jurisdiction mandates additional specific safeguards prior to a Restricted International Data Transfer, Emburse and Customer shall negotiate in good faith the implementation of the new safeguards required for compliance.

## 10. Processing of Personal Data as Related to CCPA

10.1. Data To the extent CCPA applies to any Personal Data, such Personal Data will be disclosed by Customer to Emburse for a "Business Purpose" and Emburse will act as Customer's "Service Provider" as defined by CCPA. Emburse will not retain, use, sell, rent, or disclose Personal Data for any purpose other than for the specific purpose of providing Services as described in the Agreement or as permitted or required by CCPA.

10.2. Emburse may disclose Personal Data to Emburse's service providers as needed to provide the Service contracted by Customer.

10.3. Emburse may engage service providers to fulfill Emburse's Processing obligations. In such cases, Emburse's service providers may be granted permission to Process Personal Data to the extent needed for Emburse to provide Services.

10.4. Emburse shall bind its service providers to comply with materially similar obligations to those included in this DPA.

## 11. Severance

If any provision of this DPA is held invalid or unenforceable, the parties agree that the remainder of this DPA shall remain valid and in force. Any such invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, or (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

## 12. Notices

All instructions, requests, consents, notices, and other communications under and regarding this DPA, from either party or from third parties, shall be sent or forwarded to the following representatives of Customer and Emburse as otherwise directed by this DPA and the Agreement:

Emburse: Emburse Inc., Attn: Emburse Legal Department, 320 Cumberland Ave., Portland, ME 04101 privacy@emburse.com.

Customer: Order Form Customer entity name, Attn: dept. or individual on behalf of Customer Data Privacy Officer, and Customer point of contact information under Order Form and Agreement notice terms.

## 13. Definitions

In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

13.1. "**Affiliate**" means each legal entity (other than non-operating holding companies) that is controlled by, or is or under common control with Emburse on or after the Effective

Date and for so long as such entity remains controlled by, or is under common control with Emburse or Customer (where "**controls**", in its various forms herein, means the ownership of, or the power to vote, directly or indirectly, a majority of any class of voting securities of a corporation or limited liability company, or the ownership of any general partnership interest in any general or limited partnership.

13.2. "**Authorized Affiliate**" means any Customer Affiliate which is: (i) subject to Data Protection Laws; and (ii) permitted to use the Services pursuant to the Agreement between Customer and Emburse.

13.3. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1978.00 et seq., and its implementing regulations and the California Privacy Rights and Enforcement Act of 2020.

13.4. **"CPRA"** means the California Privacy Rights Act of 2020, enhancing the protection of California residents granted by CCPA.

13.5. "**Customer**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates).

13.6. "**Data Protection Laws**" means any and all legislations protecting the Personal Data of natural persons that is applicable to the processor of Personal Data including, but not limited to, GDPR, UK GDPR, CCPA, CPRA and any legislation that supplements or amends the aforementioned.

13.7. "**GDPR**" means the 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/ED (General Data Protection Regulation).

13.8. "**Personal Data**" means any information about an individual that (i) can be used to identify, contact, or locate a specific individual, (ii) can be combined with other information that can be used to identify, contact, or locate a specific individual, or (iii) is defined as "Personal Data" or "Personal Information" by Data Protection Laws or regulations relating to the collection, use, storage, or disclosure of the information about an identifiable individual.

13.9. "**Restricted International Data Transfer**" means a transfer of Personal Data from Customer to Emburse where such transfer would be prohibited by Data Protection Laws in the absence of executed Standard Contractual Clauses.

13.10. "**Standard Contractual Clauses**" means the EEA Module 2 Controller to Processor Standard Contractual Clauses established by the Commission Implementing Decision (EU) 2021/915 of 4 June 2021. The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Addendum II.

13.11. "**Sub-processor**" means Emburse Affiliates and third parties engaged by Emburse or its Affiliates in connection with the Service and which Process Personal Data in accordance with this DPA. Sub-processors are available at https://www.emburse.com/legal/sub-processors.

13.12. "**Subscription Term**" shall have the meaning set forth in the Terms and Conditions referenced in the Order Form.

13.13. "**UK Data Protection Laws**" means United Kingdom General Data Protection Regulation ("**UK GDPR**"), the Data Protection Act 2018, and any law implementing or supplementing such legislation.

13.14. The terms "**Business Purpose**," "**Controller**," "**Data Exporter**," "**Data Importer**," "**Data Protection Impact Assessment**," "**Data Subject**," "**Personal Data Breach**," "**Processing**," "**Processor**," "**Service Provider**," "**Special Categories of Data**," and "**Supervisory Authority**" shall have the meaning described in the Data Protection Laws, and in each case their cognate terms shall be construed accordingly.

IN WITNESS WHEREOF, the Parties have caused this Data Protection Agreement to be executed by their duly authorized representatives, as of the Effective Date.

| **Emburse, Inc. for itself and on behalf of its Affiliates:** | **Customer:** |
|---|---|
| Signature: | Signature: |
| Name: | Name: |
| Title: | Title: |
| Date: | Date: |

# ADDENDUM I

## INTRODUCTION AND SCOPE

### Emburse Platform and Apps

Emburse humanizes work by empowering business travelers, finance professionals, and CFOs to eliminate manual, time-consuming tasks so they can focus on what matters most. Emburse offers a growing portfolio of award-winning expense and AP automation solutions, including Emburse Abacus, Emburse Spend, Emburse Captio, Emburse Certify, Emburse Chrome River, Emburse Cards, Emburse Nexonia, Emburse SpringAhead, Emburse Go, Emburse Analytics, Emburse Pay and Emburse Tallie.

Its innovative offerings are tailored to meet the unique needs of specific industries, company sizes, and geographies, and are trusted by more than 9 million users in more than 120 countries. Over 16,000 customers, from start-ups to global enterprises rely on Emburse to eliminate manual processes, make faster, smarter decisions, and help make users' lives - and their businesses - better. Emburse is recognized as a leader in expense management and accounts payable automation by analyst firm IDC, and has received multiple awards for its high levels of customer satisfaction.

## GOVERNANCE

### Information Security Team

Emburse has a dedicated Information Security Team consisting of Security Engineering, Security Operations, Security Programs, and IT Governance, Risk and Compliance (GRC) professionals. Emburse's Information Security takes an integrated, risk-based approach to security, leveraging automation and tools for continual evaluation of risk and compliance for new developments. Emburse's security and privacy program is certified as ISO 27001 and ISO 27701 compliant. A company-wide risk assessment is conducted annually with risks associated with the appropriate risk owner for remediation or acceptance. These are maintained within our annual risk assessment. All identified risks are treated as appropriate. Other certifications include SOC1 type II, SOC2 type II, and PCI-DSS.

### Policies, Plans, and Standards

Emburse has documented policies to meet the recommendations of the ISO 27001 and ISO 27701 standards. Emburse Information Security Policies are reviewed at least annually or as a significant change occurs to ensure its continuing suitability, adequacy and effectiveness.
In conjunction with its data center hosting providers, Emburse covers the critical security and privacy areas: physical security, network infrastructure, security operations and data handling.

- Physical security includes locking down and logging all physical access to our data centers.

- Network infrastructure provides the availability guarantees backed by our SLAs.
- Operational security involves creating business processes and policies that follow security best practices to limit access to confidential information and maintain tight security.
- Data Handling provides guidance on handling customer and employee data.

### Emburse Information Security Policies

- ISPOL01: Information Security
- ISPOL02: Acceptable Use
- ISPOL03: Data Handling
- ISPOL04: Password
- ISPOL05: Messaging & Collaboration
- ISPOL06: Cryptography & Encryption
- ISPOL07: Third Party
- ISPOL08: Network Security
- ISPOL09: Physical Security
- ISPOL10: Data Retention
- ISPOL11: Cyber Resiliency
- ISPOL12: Access Management
- ISPOL13: Asset Management
- ISPOL14: Equipment Disposal
- ISPOL15: Secure Application Development
- ISPOL16: Infrastructure Hardening

### Security Plans, Standards, and Guidelines

- ISPR01: Security Incident Response Plan
- Emburse Business Continuity Plan
- ISDRP01: Information Security Disaster Recovery Plan
- Standard Cryptography and Encryption
- ISGDL01 Security Awareness Guideline
- Password Guideline

## ACCESS CONTROL

### Standards

Emburse maintains strong access control policies that apply to employee access to all production environments. The control processes include, but are not limited to:

- Strict password complexity requirements
- Use of the Principle of Least Privilege and Segregation of Duties
- Unique user identification and authentication
- Account provisioning and deprovisioning processes
- Secure, encrypted remote access
- Multi-factor authentication

## Authentication

Emburse recommends using Single Sign On (SSO), configured with multi-factor authentication. This can be configured in the Emburse Sign-in administrative options and your SSO provider's configuration. This best of breed deployment configuration allows configuring strong authentication to Emburse and allows consistent provisioning, operating and monitoring of Emburse along with other corporate applications.

# DATA HANDLING AND PRIVACY

## Data Classification

Emburse has implemented information classification to handle data as securely as possible. Based on its sensitivity, information is classified and labeled into the following three categories:

Highly Confidential: Information that is intended for specific individuals, with a high risk of financial loss or damage to the company's reputation if unauthorized disclosure or access occurs.

Confidential: Information that is intended for limited distribution, with risk of financial loss or damage to the company's reputation if unauthorized disclosure or access occurs.

Public: Information that is publicly available and/or intended for public dissemination.

## Data Retention

All information is stored until or unless you instruct us otherwise. Upon termination, the customer is given the opportunity to export their data. Once the customer has successfully transferred their data, the customer may request that all data is purged from the system in a secure fashion.

Alternatively, customers can request that data be deleted if it exceeds their internal retention period and is not required for regulatory purposes.

## Personally Identifiable Information (PII)

All PII data stored in Emburse applications are retained and used only for the purposes of giving the users the intended service of the system. The information is not reused or sold for other purposes. The information is treated in accordance with authorized data storage plans and off-site storage of the data is managed appropriately as such. Access to PII data is limited to "need to know" employees for authorized purposes only. Storage of PII assets is limited to necessary length of time for purposes of intended workflows. Assets are limited to necessary data elements. Physical access to PII is restricted by the hosting provider's secure data center environment and proper network and hardware/software protections. There is to be no downloading, printing or otherwise storing PII assets on devices other than approved Data Center assets. Disabled user accounts cannot access PII data. An account lockout threshold is

enforced that assists with blocking unauthorized access to PII data. Access to PII data is restricted to appropriate users based on Authorization rules and system roles. Emburse Does not collect or store IP addresses, and therefore IP addresses should not be included on the list. Specifically, Emburse's marketing department does not collect IP addresses, and the product does not collect IP addresses nor store IP addresses. The product references only a portion of a user's IP address (the class C subnet) with an irreversible hash, and so Emburse is not able to regenerate the user's IP address.

# ENCRYPTION

## General Standards

- Employee Laptops - full disk AES-256 encryption
- Customer data - fully encrypted AES-256
- TLS - default is TLS 1.2 or stronger

## AWS Encryption

Amazon Web Services (AWS) instances, and volumes are encrypted using AES-256.

Encryption keys via AWS Key Management Service (KMS), are IAM role protected, and protected by AWS provided HSM certified under FIPS 140-2.

## Customer Databases

Emburse uses the multi-tenant model. With Emburse, each tenant is identified by a unique customer identifier within all systems. Each customer is given the same application code but with customer-specific configuration options that adapt the application to their own needs.

Each tenant is served using a single common instance, with configurable metadata specific to them, that is applied at run time to give each customer a unique user experience.

Customers access a load-balanced farm of multiple instances with configurable metadata and data isolation where the data of each customer is kept completely separate from all other customers. Emburse employs the Shared Database Separate Schema methodology (i.e., all client data is stored in a shared database and schema and data are separated by SQL query filters).

Emburse has structured our applications to support the operational requirements of maintainability, scalability and security by using multiple tiers. Tiers are physically partitioned from each other in separate network segments, which isolate them and provide greater security. These tiers are the 1) web layer, 2) application layer and 3) database layer.

Communications between the segments are encrypted and only permitted across limited channels. Emburse performs regular penetration tests to assure the isolation is intact.

## Key Management

Emburse provides full AES 256-bit encryption at rest. Databases reside on encrypted Amazon Elastic Block Store (EBS) volumes. Images and other archives utilize encrypted Amazon Web Services (AWS) S3 buckets. We employ AWS Key Management Service to provide key management and key rotation. All keys are rotated at least annually.

# NETWORK SECURITY

## Segmentation

Emburse has structured our applications to support the operational requirements of maintainability, scalability and security by using multiple tiers. Tiers are physically partitioned from each other in separate network segments, which isolate them and provide greater security. These tiers are the 1) web layer, 2) application layer and 3) database layer. Communications between the segments are encrypted and only permitted across limited channels. Emburse performs regular penetration tests to assure the isolation is intact.

## Firewalls

Emburse employs stateful firewalls at the edge and host-based firewalls on the interior. Emburse and our hosting environments provide logical and physical security for the service and its related systems, including firewalls, load balancers, routers, network switches and operating systems.

AWS provides Emburse with the flexibility to place instances and store data within multiple geographic regions, as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone, meaning availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region).
In addition to discrete uninterruptible power supply (UPS) and onsite backup generation facilities, availability zones are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

Emburse has architected our AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of failure, including natural disasters and system failures.

## Data Segregation

Emburse customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. Significant measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer.

Emburse's access control policies are based on the principles of "least privilege" and "segregation of duties." Segregation is enforced through role-based access control (RBAC) policies and technical controls. Emburse maintains four environments:

1. Production
2. UAT (QA environment provided to all customers for the term of their agreement; treated as production environment for compliance and segregation of duties) *
3. Internal QA (staging)
4. Development Engineers are not permitted access to any production environments, including UAT.

Engineers are not permitted access to any production environments, including UAT.

**Nexonia: UAT does not exist.*

# PLATFORM HARDENING

## Denial of Service (DoS) Protections

Emburse is protected by Amazon Web Services (AWS), one of the most resilient, high-availability cloud providers in the world, who provides DoS and DDoS protections of many kinds of network-layer attacks. Emburse leverages Amazon Shield for advanced and automatic DDoS protections.

## Vulnerability Scanning and Penetration Testing

Emburse runs vulnerability scanning monthly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). Annual penetration testing, by an approved and independent third party.

We perform penetration testing on network infrastructure and applications at least annually and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment).

Network segmentation is conducted twice per year.

Penetration Test Results Executive Summary are available on request subject to NDA.

In addition, Emburse has a private Bug Bounty program. Emburse and the security of the platform are tested on a continuous basis.

## Web Application Firewall

Emburse has deployed and manages an Web Application Firewall (WAF), in addition to the network-based firewalls. This additional security control prevents many known attack patterns.

## Endpoint Protection: Malware and Antivirus

Emburse has deployed endpoints protections through the use of the anti-malware software across all Emburse systems. Malware detection runs continuously and comprehensive scans are done on a regular basis. Emburse has implemented CrowdStrike for workstation and server protection and has contracted incident response for anomalous activity. Networks and emails are monitored for illicit file movement and movement of confidential data. Anti-virus and anti-malware are installed on all workstations and servers.

# PATCHING AND VULNERABILITY MANAGEMENT

## Patching

We follow an agile development model with system updates deployed every two weeks. These biweekly updates install without downtime and with minimal impact to end users. These updates include patches and bug fixes, as well as new product functionality and system performance tuning.
All high or critical vulnerabilities are patched within 30 days. Medium vulnerabilities are patched within 90 days.

## Vulnerabilities

Emburse uses scanners to monitor the production environment for vulnerabilities and misconfigurations. Vulnerability scans are performed regularly. Newly discovered security vulnerabilities are assessed, mitigated and remediated based on impact. The Security and Operations team meets weekly to review new Common Vulnerabilities and Exposures (CVE) across all systems in the environment.

Emburse participates in a Bug Bounty program. Findings disclosed by security researchers are assessed, mitigated and remediated based on impact.

Emburse Information Security Team members regularly monitor threat feeds, vulnerability platforms or databases, and other security information sources for up-to-date information on emerging threats, vulnerabilities, and exploits.

# CHANGE AND RISK MANAGEMENT

## Change Management Policy and Process

Emburse change management processes apply to changes made to the platform and infrastructure. The process requires, but is not limited to:

- Developers are identified and authorized
- Source code changes are reviewed and approved
- Source code changes pass tests

- Roll-back procedures exist
- Segregation of duties in deployment
- Logically separated development, staging, and production environments
- All changes are logged
- Emergency changes require approval

## Security Reviews

Emburse conducts regular security stakeholder review meetings on a regular basis to discuss and track potential or active risks related to the business. The review is sponsored and led by the Information Security Team and generally attended by Chief Product Officer, Chief Technical Officer, VP of Operations Engineering, Directors, and management or program management from all business units, as appropriate. The attendees regularly review business, legal or regulatory, and technical risks, and potential impacts outside of formal meetings.

## Third Party Risk: Vendor and Partner Management

Emburse performs a risk analysis on third-party service providers. Emburse senior management recognizes that secure, dependable relationships with third parties are necessary to support the company's products and services. These policies and procedures apply to third parties regardless of the country in which they are based or from where the services are provided.

Senior management further recognizes that third-party relationships present potential risks that must be properly managed, beginning with a sound due diligence process at the outset and continuing with annual or more frequent reviews of all third-party relationships. The extent of risk varies with each third-party relationship; among the most common third party-related risks are lack of third-party oversight by senior management, which could result in the company experiencing operational risks, privacy risks and reputation risks.

Senior management recognizes that it is ultimately responsible for identifying and controlling the risks arising from such relationships, to the same extent as if they were handled within the company. The security review and threat modeling can include, but is not limited to:

- Reviews of data flow or technical diagrams
- Risk assessments related to data handling and measures taken to protect data
- Other third-party integrations
- Compliance reporting
- Access controls and requirements
- Penetration testing results
- Hosting models
- Sandbox testing or security testing performed by Emburse's Information Security Team

## Security Awareness & Privacy Training

All Emburse employees are required to complete Security Awareness training on hire and every year thereafter. The training includes data privacy and governance, data protection, confidentiality, social engineering, password policies, and overall security responsibilities inside and outside of Emburse. As part of the Security Awareness a privacy training, employees must acknowledge completion and accept their part of maintaining the overall security and privacy of Emburse.

Developers are trained annually, so as to maintain knowledge of the OWASP Top 10 for secure code development. Finally, Emburse conducts regular phishing tests. Those who click on a simulated phishing email are to take remedial training.

# RESILIENCY: INCIDENT RESPONSE, BCP, AND DR

## Incident Response

Emburse's Incident Response Policy encompasses four principal phases: 1) preparation, 2) detection and analysis, 3) containment, eradication and recovery and 4) post-incident activity. When an incident is suspected, the appropriate resources are dedicated to validation and remediation. Depending on who reported the issue and how it is handled, the responsibility for remediation will lie with either the Emburse support or operations teams.

The Security Incident Response Team (SIRT) Lead acts as the coordinator in response to all major security-related incidents or weaknesses. A major security incident or weakness is considered to be an impact to confidentiality (e.g., exfiltration of encryption keys), integrity (e.g., unanticipated data leakage or exfiltration), or availability (e.g., severe degradation of performance). The Incident Response Team Lead is responsible for assigning staff to work on specific tasks of the incident handling process and coordinating the overall incident response.

All personnel involved in incident response and remediation are responsible for providing any needed information to members of the Incident Response Team. Any directives given by a member of the Security Incident Response Team may supersede the specifics of this policy.

## BCP/DR

Emburse conducts a business risk analysis annually to evaluate and determine critical business processes and systems for all business functions. This includes an inventory of critical systems, measuring the overall potential operational impact of critical system disruption and assigning an appropriate RTO and RPO metric based on that criticality. All backups are encrypted.

The detection of a disruption or disaster that could affect Emburse operations or application services is the responsibility of the Security Incident Response Team (SIRT). The specific responsibilities of the SIRT and associated groups are outlined in our ISO-certified Business Continuity Plan.

The SIRT is automatically updated through monitoring services that provide notifications through email and phone. When a disruption or disaster occurs, the on-call SIRT member immediately makes an assessment of affected services. If necessary, they initiate the Disaster Recovery Plan and notify the other members of the Disaster Recovery Team (DRT).

## Tabletop

Emburse conducts an annual tabletop exercise with a cross-functional group of employees from all departments of the organization. This annual event is structured to test the readiness of the

team for response to a production event. The exercises require participants to test, record, and simulate response activities in the event that the tabletop was an actual emergency. An after action review and lessons learned are conducted to ensure continuous improvement.

## Resiliency Policy

Emburse Resilience Policy governs and enforces processes including, but not limited to:

- Backup scheduling and monitoring
- System restoration
- Encryption in transit and at rest
- Engineering responsibilities

Emburse customer content and data are highly available and backed up daily. Any data at rest and in transit is encrypted. Logging is enabled to track backup status. Emburse backs up to a segmented, independent cloud account and is kept unavailable (offline) to the rest of production systems and engineers.

## Monitoring and Alerting

Emburse performs 24x7x365 monitoring of the Emburse infrastructure and environments. Automated monitoring and alerting for performance (e.g. uptime, CPU, memory, disks) and security is in place and monitored.

Monitoring for misuse is performed across all production infrastructure to detect and alert suspicious activity or changes to critical infrastructure.

## RTO/RPO

Emburse strives to keep services up and running; however all SaaS companies suffer occasional disruptions and outages. Recovery time objectives (RTO) and recovery point objectives (RPO) are tied to specific processes, not general availability of the entire platform. These metrics are evaluated annually during Emburse business risk analysis. Emburse maintains near-real time backups, therefore, the general RPO is measured in minutes.

# COMPLIANCE

## Emburse

Emburse and its subsidiaries are compliant with multiple security and compliance frameworks including SOC1, SOC 2, ISO 27001, and PCI-DSS.

SOC 1, Many of Emburse's subsidiaries have been audited by a third-party and have achieved certified SOC 1 compliance. The report is available under NDA for customers or prospective customers to review.

SOC 2, Many of Emburse's subsidiaries have been audited by a third-party and have achieved certified SOC 2 compliance. The report is available under NDA for customers or prospective customers to review.

ISO 27001, Emburse has been audited by a third-party and has achieved certified ISO 27001 security compliance. The certificate of registration is available under NDA for customers or prospective customers to review.

ISO 27701, Emburse has been audited by a third-party and has achieved certified ISO 27701 privacy compliance. The certificate of registration is available under NDA for customers or prospective customers to review.

PCI-DSS, Many of Emburse's subsidiaries have been audited by a third-party and have achieved PCI-DSS compliance. The certificate of registration is available under NDA for customers or prospective customers to review.

GDPR and Schrems II Ruling, Emburse's Privacy Policy and GDPR Data Privacy information can be found here: https://www.emburse.com/privacy-policy

## Amazon Web Services

AWS compliance can be found here: https://www.atlas.aws/

# ADDENDUM II

## STANDARD CONTRACTUAL CLAUSES

Controller to Processor (Module 2)

**SECTION I**

***Clause 1***

**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

***Clause 2***

**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3***

**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***Clause 4***

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5***

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6***

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7 – Optional***

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

***Clause 8***

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### 8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the

competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

***Clause 9***

**Use of sub-processors**

(a) ~~OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.~~

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(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 sub-processors at least **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 sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

***Clause 10***

**Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

***Clause 11***

**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

~~[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]~~

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

***Clause 12***

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

***Clause 13***

**Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects

whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

### *Clause 14*

### Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

***Clause 15***

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

***Clause 16***

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

***Clause 17***

**Governing law**

**[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany (*specify Member State*).]**

~~[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 another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]~~

***Clause 18***

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of **Germany** (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

## ANNEX I

### A. LIST OF 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]*

**The contact information shall be the information appearing in the the Order Form**

Name: ***See Order Form***

Address: ***See Order Form***

Contact person's name, position and contact details: ***See Order Form***

Activities relevant to the data transferred under these Clauses:

***The Customer of Emburse's services as described in the Order Form***

Signature and date: ***The signature and date appearing in the Data Processing Agreement or Order Form, as applicable, is hereby incorporated into these SCCs***

Role (controller/processor): ***Controller***

2. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: ***Emburse, Inc.***

Address: ***Emburse Legal Department, 320 Cumberland Ave., Portland, ME 04101 privacy@emburse.com.***

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 in Order Form***

Signature and date: ***The signature and date appearing in the Data Processing Agreement or Order Form, as applicable, is hereby incorporated into these SCCs***

Role (controller/processor): ***Processor***

2. …

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

***Customer's employees***

*Categories of personal data transferred*

*…*

*Sensitive data transferred (if applicable) and 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.*

***Not Applicable***

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

***Continuous***

*Nature of the processing*

***As described in the Order Form***

*Purpose(s) of the data transfer and further processing*

***As needed to provide the services in the Order Form***

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

***90 days and as needed to fulfill contractual and regulatory obligations***

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

***As described in Emburse Subprocessor website***

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*…*

***As described in Section 9.1.5.4 of the DPA***

---

**ANNEX II**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

***As described in Addendum I (please see supra)***

…

---

**ANNEX III**

**LIST OF SUB-PROCESSORS**

***Available at https://www.emburse.com/legal/sub-processors or as attached to this DPA***

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

# ADDENDUM III

## IDTA

## 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**

| | | |
|---|---|---|
| **Start date** | | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | ***As stated in the Order Form*** | Full legal name: ***Emburse, Inc.***<br>Trading name (if different):<br>Main address (if a company registered address): ***Emburse Legal Department, 320 Cumberland Ave., Portland, ME 04101 privacy@emburse.com.***<br>Official registration number (if any) (company number or similar identifier): |
| **Key Contact** | ***As stated in the Order Form*** | Full Name (optional): ***Bill Bowman***<br>Job Title: ***DPO***<br>Contact details including email: |

| | | |
|---|---|---|
| | | ***privacy@emburse.com*** |
| **Signature (if required for the purposes of Section 2)** | | |

**Table 2: Selected SCCs, Modules and Selected Clauses**

| | |
|---|---|
| **Addendum EU SCCs** | ***The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:*** |

| Module | Module in operation | Clause 7 (Docking Clause) | Clause 11 (Option) | Clause 9a (Prior Authorisation or General Authorisation) | Clause 9a (Time period) | Is personal data received from the Importer combined with personal data collected by the Exporter? |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | ***Module Two (Controller to*** | ***Y*** | ***N*** | ***Option 2: General Authorization*** | ***30 days*** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ***Processor )*** | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |

**Table 3: Appendix Information**

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

Annex 1A: List of Parties: ***As described in Annex I of Addendum II***

Annex 1B: Description of Transfer: ***As described in Annex I of Addendum II***

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: ***As described Addendum I***

Annex III: List of Sub processors (Modules 2 and 3 only): ***Available at https://www.emburse.com/legal/sub-processors or as incorporated to this order form***

**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:<br>Importer<br>Exporter<br>**neither Party** |

# 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 fulfills 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.

## Alternative Part 2 Mandatory Clauses:

| | |
|---|---|
| **Mandatory Clauses** | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. |