Data Processing Addendum

This Data Processing Addendum, including its Appendices ("DPA"), forms part of the Terms and Conditions or other written or electronic agreement for the purchase of Emburse services (the "Principal Agreement"). This DPA applies to Personal Data processed by Emburse and its Subprocessors in connection with its provision of the Service. For purposes of this DPA, the Emburse entity that is the party to the executed Order Form with Customer under the Principal Agreement is the party to this DPA and shall be the Data Importer.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Emburse processes Personal Data for which such Authorized Affiliates qualify as the Controller. For purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

If in the course of providing the Services to Customer pursuant to the Principal Agreement, Emburse may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

1. Structure

1.1 Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

1.2 The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer, and those Authorized Affiliates that it permits to use the Service, act as the Controller and Emburse acts as the Processor. Customer shall act as a single point of contact and is solely responsible for obtaining any relevant authorizations, consent, instructions or permissions for the Processing of Personal Data in accordance with this DPA, including, where applicable, approval by Controllers to use Emburse as a Processor. Where authorizations, consent, instructions, or permissions are provided by Customer, these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Service. Where Emburse informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Service. It shall be Customer's responsibility to forward such information and notices to the relevant Controllers.

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

2. Processing of Personal Data

2.1 Emburse will Process Personal Data on behalf of and only in accordance with Customer's documented instructions. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Service then constitutes further instructions. Emburse will use reasonable efforts to comply with other documented instructions provided by Customer where such instructions are consistent with the terms of the Agreement, are required by Data Protection Laws and do not require changes to the Service.

2.1.1 If Emburse is unable to comply with an instruction or such instruction infringes Data Protection Laws, in Emburse's reasonable opinion, Emburse shall promptly notify Customer.

2.1.2 Emburse may also Process Personal Data where required to do so by applicable law. In such case, Emburse will inform Customer of that legal requirement unless that law prohibits such information on important grounds of public interest.

2.2 Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Emburse as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from disclosures of Personal Data, including the sale of Personal Data under the CCPA.

3. Personnel

Emburse and its Sub-processors shall take reasonable steps to ensure the reliability of any employee, agent or contractor who have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or have access to the relevant Personal Data. Emburse shall ensure all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Emburse and its Sub-processors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4. Data Subject Rights

4.1 Emburse shall, to the extent legally permitted, 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 (each a "Data Subject Request") without itself responding to such request. Taking into account the nature of the Processing, Emburse shall reasonably cooperate with Customer and Controllers in dealing with Data Subject Requests by appropriate technical and organizational measures, in so far as this is possible.

4.2 Emburse shall:

4.2.1 not disclose Customer Personal Data to any third party other than approved Emburse Affiliates and Sub-Processors without the Customer's prior written consent other than to the extent required by a regulator or court of law.

4.2.2 to the extent permitted by applicable Law, not deal with regulators, law enforcement agencies, the relevant individuals concerned or media in respect of the Personal Data without the Customer's prior written consent;

4.2.3 promptly notify the Customer of any complaint received by Emburse regarding Personal Data practices, or of any request or enquiry from a government body or regulator having jurisdiction under Data Protection Laws and cooperate with the Customer in the resolution of any such complaint or any investigation or enforcement action by such a government body or regulator.

4.3 In the event of requests from a non-EU Responsible Authority to disclose Customer Personal Data on a voluntary basis, Emburse agrees that it shall refrain from disclosing any Customer Personal Data unless it has obtained the express consent of the Customer or the relevant Data Subject(s).

4.4 In the event that Emburse receives a formal disclosure order for Customer Personal Data from a non-EU Responsible Authority, Emburse will provide Customer with prompt written notice, unless providing such notice would breach applicable Law or regulation (in such instances Emburse will challenge the legality of any such order itself and wherever possible seek interim measures to suspend the effects of the order until a court has decided on the merits), so that Customer may seek a protective order or other appropriate remedy. If Customer seeks such a protective order, Emburse will provide such cooperation as Customer reasonably requests. In the event that such a protective order or other remedy is not obtained (either by Customer or by Emburse), Emburse agrees that it will not disclose the Customer Personal Data requested until required to do so under the applicable procedural rules and will provide only the minimum amount of Customer Personal Data that is permissible.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Emburse shall maintain appropriate technical and organizational measures for the protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in Appendix 2, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. Emburse will regularly monitor compliance with these measures.

5.2 Emburse may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

6. Sub-processors

6.1 Customer acknowledges and agrees that: (a) Emburse Affiliates may be retained as Sub-processors; and (b) Emburse and Emburse Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

6.1.1 Any third party Sub-Processors shall be engaged under a written (including electronic form) contract containing data protection obligations no less protective than those in this Agreement with respect to the protection of Personal Data, to the extent applicable to the services provided by such Sub-Processor.

6.1.2 For any Sub-processor, Emburse will carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Personal Data required by the Principal Agreement.

6.1.3 Emburse will make available to Customer, upon request, a list of Sub-processors in place on the effective date of the Agreement, including the name, address, and role of each Sub-processor Emburse uses to provide the Service.

6.2 Emburse's use of Sub-Processors is at its discretion, provided that:

6.2.1 Emburse will inform Customer of the appointment of any new Sub-processor in advance (by email or by making such information available on an website accessible to Customer), including full details of the Processing to be undertaken by the Sub-processor.

6.2.2 If, within ten (10) business days of receipt of that notice, Customer notifies Emburse in writing of a legitimate reason under Data Protection Law to object to the proposed appointment, Emburse shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor.

6.2.3 If Emburse is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days from receipt of Customer's notice, Customer may terminate the Order Form with respect to the Services which require the use of the proposed Sub-processor by providing written notice to Emburse received no later than ninety (90) days from date of Emburse's notice of such proposed Sub-processor. If Customer does not terminate within such ninety (90) day period, Customer is deemed to have accepted the new Sub-processor. Any termination under this Section 6.2.3 will be without fault by either party and shall be subject to the terms of the Agreement.

6.3 Emburse will be liable for the acts and omissions of its Sub-processors to the same extent Emburse would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6.4 Emburse may replace a Sub-processor without advance notice where the reason for such change is outside of Emburse's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Emburse will inform Customer of the replacement Sub-processor as soon as reasonably practicable following its appointment and 6.2.2 and 6.2.3 will apply.

7. Personal Data Incident Management

7.1 Emburse shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Emburse shall cooperate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

If required by Data Protection Law, Emburse shall provide reasonable assistance and cooperation to fulfill Controller's obligation to carry out a data protection impact assessment, or prior consultation with a Supervisory Authority, which are required under the GDPR or equivalent provisions of any other Data Protection Law solely in relation to Customer's use of the Service and to the extent Customer does not otherwise have access to the relevant information and such information is available to Emburse.

9. Deletion or return of Personal Data

9.1 Subject to this Section 9, Emburse shall, to the extent allowed by applicable law, promptly and in any event within ninety (90) days of the date of cessation of the Services involving the Processing of Personal Data (the "Cessation Date"), delete and procure the deletion, anonymization or pseudonymization of all copies of such Personal Data. Certification of the destruction as provided in this Section 9 shall be provided upon Customer's request.

9.2 During the term of the Agreement, Customer will have access its Personal Data at any time and can export and retrieve such data in a standard format. Export and retrieval may be subject to technical limitations. If export and retrieval as described in the foregoing is not reasonably possible, Emburse and Customer will find a reasonable method to allow Customer to access the Personal Data. Upon written request to Emburse within thirty (30) days of the Cessation Date, Emburse will permit Customer access to the Services for thirty (30) days the sole purpose of exporting all Personal Data.

9.3 Emburse may retain the Personal Data to the extent and only for such period of time as required by Applicable Laws. Emburse shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws.

10. Certifications and Audits

10.1 Emburse will, upon written request of Customer, make available evidence of its compliance with the technical and organizational measures that protect the Service through third-party certifications and audits as described in the security Documentation.

10.2 Customer, a Controller, or its respective independent third party auditor reasonably acceptable to Emburse, may have a right to audit Emburse's control environment and security practices relevant to the Processing if:

10.2.1 Emburse fails to provide sufficient evidence under Section 10.1;

10.2.2 An audit is requested by Customer's, or a Controller's, relevant data protection authority; or

10.2.3 Data Protection Law provides Customer with a direct audit right, provided any such audit shall only occur once in any twelve (12) month period unless such law requires more frequent audits.

10.3 If a Controller (other than Customer) requests to conduct an audit under section 10.2, such audit must be undertaken by and through Customer unless Data Protection Law requires otherwise. If several Controllers whose Personal Data is processed Emburse under the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits. Customer shall bear the costs of all audits under this Section 10.

10.4 Customer or the relevant Controller undertaking an audit under Section 10.2 shall give Emburse at least sixty (60) days (or such other period as required by Data Protection Law) prior notice of any audit to be conducted under section 10.2. The scope of any audits shall be mutually agreed by the parties acting reasonably and in good faith. Audits shall be limited to three (3) days and Customer (or relevant Controller) shall make (and ensure that each of its auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to Emburse premises, equipment, personnel and business in the course of such audit. Customer shall bear the costs of such audit and will provide the results of any audit to Emburse. If an audit determines that Emburse has breached its obligations under the DPA, Emburse will promptly remedy the breach at its own cost.

10.5 To the extent the Standard Contractual Clauses apply to this DPA as set forth in Section 11 below, the parties agree that audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the provisions of this Section 10.

11. Data Transfers

11.1 Personal Data that Emburse processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Emburse or its Subprocessors operate. Customer appoints Emburse to perform any such transfer of Customer Data and Personal Data to any such country and to store and process Customer Data and Personal Data to provide the Services. All transfers of Customer Data out of the European Union, European Economic Area, and Switzerland by the Services will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

11.2 The EU Standard Contractual Clauses set forth in (Appendix 3) to this DPA (the "EU SCCs") shall apply to all Emburse subsidiaries or Affiliates and to: (i) Customer which is subject to the data protection laws of the European Union, The European Economic Area and/or their member states, and/or Switzerland, and (ii) its Authorized Affiliates. Each of the foregoing shall be deemed "data exporters" for the EU SCCs. In the event of any conflict or inconsistency between the body of this DPA (including Appendices 1 and 2) and the EU SCCs in Appendix 3, the EU SCCs shall prevail.

11.3 The UK Standard Contractual Clauses set forth in (Appendix 4) to this DPA (the "UK SCCs") shall apply to all Emburse subsidiaries or Affiliates and to: (i) Customer which is subject to the

data protection laws of the United Kingdom, and (ii) its Authorized Affiliates. Each of the foregoing shall be deemed "data exporters" for the UK SCCs. In the event of any conflict or inconsistency between the body of this DPA (including Appendices 1 and 2) and the UK SCCs in Appendix 4, the UK SCCs shall prevail.

12. Severance

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (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, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

13. Definitions

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

13.1.1 "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.

13.1.2 "Authorized Affiliate" means any Customer Affiliate which: (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland, and/or United Kingdom; and (b) is permitted to use the Services pursuant to the Agreement between Customer and Emburse.

13.1.3 "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1978.00 et seq., and its implementing regulations.

13.1.4 "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

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

13.1.6 "Customer Data" has the meaning set forth in the Agreement as "Customer Data" provided that such data is electronic data and information submitted by or for Customer in the Service.

13.1.7 "Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including EU Data Protection Laws and UK Data Protection Laws, to the extent applicable, and the data protection or privacy laws of any other country.

13.1.8 **“Data Subject” means, unless otherwise defined in Data Protection Laws, an identified or identifiable natural person that is the subject of Personal Data.**

13.1.9 **"EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.**

13.1.10 **"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).**

13.1.11 **“Personal Data" means any information related to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable data under applicable Data Protection Laws), where for each (i) or (ii), such data is Customer Data.**

13.1.12 **“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.**

13.1.13 **“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.**

13.1.14 **“Processor” means the entity which Processes Personal Data on behalf of the Controller, including as applicable, any ‘service provider’ as that term is defined by the CCPA.**

13.1.15 **“Responsible Authority” means any country's government, any institution of the European Union, and any ministry, department, political subdivision, instrumentality, authority (local or otherwise), agency, corporation, court or commission under the direct or indirect control of such country or the European Union, whether engaged in legislative, executive, regulatory, administrative or judicial functions or at any time with jurisdiction or de facto control over the parties, and/or this Agreement.**

13.1.16 **"Standard Contractual Clauses" means: (i) the EU Standard Contractual Clauses (Processors) approved by the Commission Decision of 5 February 2010, as amended by EU Commission Implementing Decision 2016/2297 of 16 December 2016 or any subsequent version thereof published by the European Commission; and (ii) the UK Standard Contractual Clauses as incorporated into UK Data Protection Law by virtue of paragraph 7 of Schedule 20 to the UK DPA 2018 and such data protection clauses as may be adopted by the UK in accordance with the procedures set out in Section 119A of the UK DPA 2018. The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Annex 4.**

13.1.17 **"Subprocessor" means Emburse Affiliates and third parties engaged by Emburse or Emburse Affiliates in connection with the Service and which Process Personal Data in accordance with this DPA.**

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

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above

Customer _____

Signature _____

Name _____

Title _____

Date Signed _____

Appendix 1 to the DPA and, if applicable, Annex I to the EU Standard Contractual Clauses

and the UK Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer to subscribed to the Service that allows Authorized Users to enter, amend, user, delete or otherwise Process Personal Data. Where the Customer allows other Controllers to also use the Service, these other Controllers are also Data Exporters.

Data Importer

Emburse is a provider of services for travel booking and management, expense tracking and management, time tracking and management, and vendor procurement and invoice management for which Emburse processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement

Duration of Processing

Subject to Section 9 of the DPA, Emburse will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Data Subjects

Unless provided otherwise by the Data Exporter, the Personal Data transferred hereunder relates to the following categories of Data Subjects: Authorized Users provided access to use the Services by Customer, employees, contractors, business partners or other individuals having Personal Data Processed by the Service

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer may submit Personal Data to the Services, the extent of which is determined by the Customer per the Service that is subscribed.. Customer can configure data fields during the implementation of the Service or as otherwise provided by the Service. The transferred Personal Data typically relates to the following categories of data: Name, email, phone number, address, system access/usage/authorization data, company name, invoice data, and application-specific data that Authorized Users enter into the data and may include employee ID, payroll ID, bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: as set out in the Agreement, if any.

Processing Operations / Purposes

The Personal Data is subject to the following basic processing activities:

- **Use of the Personal Data to setup, operate, monitor and provide the Service (including technical support)**
- **Provision of professional services**
- **Communication with Authorized Users**
- **Storage of Personal Data in designated data centers**

- **Uploads of updates or upgrades to the Service**
- **Back up of Personal Data**
- **Processing of Personal Data, including transmission, retrieval, and access**
- **Execution of instructions of Customer in accordance with the Agreement**

Appendix 2 to the DPA and, if applicable, Annex II to the EU Standard Contractual Clauses

and the UK Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in for the Processing of Personal Data:

Data Importer will maintain administrative, technical, and physical safeguards for protection of the security, integrity, and confidentiality of Personal Data Processed by the Service as further described in the Service documentation. Such safeguards include, without limitation, firewalls, SSL certificates, web application firewalls, secure development lifecycle management, secure coding practices, PCI DSS compliance, SOC 2 Type II audit, third party vulnerability assessments, internal vulnerability assessments, continuous employee education, virus/malware scanning, phishing protection, and more. Data Importer will not materially diminish the overall security of the Service during the term of the Agreement.

Appendix 3: EU Standard Contractual Clauses

Controller to Processor

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Customer, on behalf of itself and the other Controllers
(hereinafter referred to as the "data exporter")

and

Emburse
(hereinafter referred to as the "data importer")

each a "Party"; together "the Parties",

HAVE AGREED on the following Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

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 (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 (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.**

(d) **The Appendix to the parties' Data Processing Agreement (and 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.

Clause 7

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.

(b) Once it has completed the Appendix and signed Annex I, 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.

(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, 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. 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.

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) 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 [*Specify time period*] 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.

(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, 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, 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, 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 ([4]);**
- **(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

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 Germany.

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.

(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.

[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.**

APPENDIX TO EU STANDARD CONTRACTUAL CLAUSES

Annex I and II of these standard contractual clauses are contained in Appendices 1 and 2 of the parties' Data Processing Agreement (above) respectively.

APPENDIX 4: UK STANDARD CONTRACTUAL CLAUSES

Name of the data exporting organisation:

Customer, on behalf of itself and the other Controllers
(hereinafter referred to as the "data exporter")

and

Emburse
(hereinafter referred to as the "data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1. Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3. Third-party beneficiary clause

1. **The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.**
2. **The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.**
3. **The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.**
4. **The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.**

Clause 4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) **that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;**

(b) **that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;**

(c) **that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;**

(d) **that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;**

(e) **that it will ensure compliance with the security measures;**

(f) **that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;**

(g) **to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;**

(h) **to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses,**

unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses;

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6. Liability

1. **The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.**
2. **If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.**
3. **The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.**
4. **If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.**

Clause 7. Mediation and jurisdiction

1. **The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:**
   (a) **to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;**
   (b) **to refer the dispute to the courts in the Member State in which the data exporter is established.**
2. **The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.**

Clause 8. Cooperation with supervisory authorities

1. **The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.**
2. **The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.**
3. **The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).**

Clause 9. Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11. Sub-processing

1. **The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.**
2. **The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.**
3. **The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.**
4. **The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.**

Clause 12. Obligation after termination

1. **The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.**

2. **The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.**