Data Processing Addendum

This Data Processing Addendum, including its Schedules and Appendices ("**DPA**") forms part of the Terms and Conditions or other written or electronic agreement for the purchase of Emburse services (the "Agreement"). This DPA applies to Personal Data processed by Emburse and its Subprocessors in connection with its provision of the Service.

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 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. For purposes of this DPA, the Emburse entity that is the party to the executed Order Form with Customer is the party to this DPA.

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

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.

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 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 co-operate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

If, pursuant to 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 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 30 days of the Cessation Date, Emburse will permit Customer access to the Services for 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 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 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 Emburse makes available the transfer mechanisms listed below which shall apply to any transfers described in Section 11.1 above. In the event that the Services are covered by more than one transfer mechanism, they shall apply in the order set forth below.

11.2.1 The EU-U.S. and Swiss-U.S. Privacy Shield self-certifications apply subject to and as described in this Section 11.2.1. Emburse subsidiaries Certify, Inc. and Chrome River Technologies, Inc. self-certify to and comply with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, as administered by the US Department of Commerce. Emburse agrees to notify Customer in the event that it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

11.2.2 The Standard Contractual Clauses set forth in (**Appendix 3**) to this DPA (the "SCCs") apply to all other 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, Switzerland, and/or the United Kingdom, and (ii) its Authorized Affiliates. Each of the foregoing shall be deemed "data exporters" for the SCCs. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the SCCs) and the SCCs in Schedule 3, the 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 an entity that directly or indirectly controls, is controlled by or is or under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect power to direct or cause the direction of the management and policies of the subject entity, whether through ownership of more than 50% of the voting interests, by contract or otherwise;

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. 0

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, to the extent applicable, the data protection or privacy laws of any other country;

13.1.8 "**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;

13.1.9 "**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);

13.1.10 **“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;

13.1.11 “**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.

13.1.12 “**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;

13.1.13 "**Standard Contractual Clauses**" means the Standard Contractual Clauses (Processors) or any subseque3nt version thereof published by the European Commission. The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Annex 2;

13.1.14 "**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.

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, the 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, the 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.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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.

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 subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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

subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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; and

(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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor,

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
Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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 subprocessing 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 the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor 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 subprocessor 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.