

Data Processing Addendum

This Data Processing Addendum (“DPA”) supplements, is a schedule to and is incorporated into the terms of the Services Agreement (“Agreement”) between Compute Software, Inc. (“Compute Software”) and its customer (“Customer”) with regard to Compute Software’s Processing of Personal Data on behalf of Customer in accordance with the requirements of Applicable Data Protection Laws. This DPA will apply to the Processing of Personal Data by Compute Software in the course of providing the Compute Software software as a service solution (the “Services”). Compute Software and Customer may be referred to herein collectively as the “Parties”. This DPA does not otherwise disturb or impact any other agreement by and between the Parties. The Parties agree as follows:

1. Process Personal Data as Instructed

1.1 Except to the extent otherwise expressly stated in the Agreement: (i) Customer is the Data Controller of Personal Data provided in the context of the Services; (ii) Customer hereby appoints Compute Software as a Data Processor to Process such Personal Data; (iii) Compute Software shall Process Personal Data as a Data Processor as necessary to perform its obligations under the Agreement (including any Order thereunder) and otherwise strictly in accordance with the written instructions of Customer, except where otherwise required by any applicable law.

1.2 The Parties agree that the subject-matter and duration of Processing performed by Data Processor under this DPA, including the nature and purpose of Processing, the type of Personal Data, and categories of Data Subjects, shall be as described in Exhibit A of this DPA and in the Agreement.

1.3 In the event that Compute Software is otherwise required to Process Personal Data by applicable law, Compute Software will notify Customer without undue delay and the parties will cooperate to ensure that Personal Data is processed to the minimum extent required by applicable law, unless such notification is prohibited by applicable law on important grounds of public interest.

2. Confidentiality Restrictions

2.1 Compute Software shall ensure that any persons authorised to Process the Personal Data by it (including its employees, contractors, agents and subcontractors) have committed themselves to obligations of confidentiality which are at least commensurate with the confidentiality obligations contained in the Agreement or are under an appropriate statutory obligation of confidentiality; further Compute Software shall refer to Customer all requests for access to, amendment of, or deletion of Personal Data and any complaints by third parties regarding the handling of such Personal Data.

3. Security Measures

3.1 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, Compute Software shall implement appropriate technical and organizational security measures which are designed to ensure against (a) unauthorized access to, (b) unauthorized or unlawful alteration, disclosure, destruction or other unauthorized or unlawful Processing of, (c) accidental loss or destruction of, or (d) damage to, the Personal Data.

3.2 Such technical and organizational security measures shall include as appropriate and without limitation (i) industry standard measures to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, (ii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and (iii) a Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. A summary of such technical and organizational security measures is set forth in the Compute Software Information Security Framework available at <https://www.computesoftware.com/terms/>.

4. Data Subjects

4.1 Taking into account the nature of the Processing, Compute Software shall at all times cooperate with and assist Customer in so far as possible to enable Customer to meet applicable deadlines and requirements under Applicable Data Protection Laws in relation to a Data Subject's right (i) of rectification of Personal Data, (ii) of erasure of Personal Data, (iii) to restriction of Processing of Personal Data, (iv) to portability of Personal Data, (v) to object to the lawfulness of the Processing of Personal Data, and (vi) to not be subject to a decision based solely on automated Processing.

4.2 Compute Software shall notify Customer, as soon as possible, of any request made by a Data Subject to access Personal Data and shall at all times cooperate with and provide Customer with any assistance it may require in order to execute Customer's obligations under Applicable Data Protection Laws.

5. Notification of Security Incident

5.1 In the case of a Personal Data Breach, Compute Software shall promptly, without undue delay, notify Customer of the Personal Data Breach. To the extent that Compute Software has access to such information at the time of the notification, such notification shall (i) describe the nature of the Personal Data Breach, without limitation, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) describe the likely consequences of the Personal Data Breach, and (iii) describe the measures proposed to be taken by Compute Software to address the Personal Data Breach (provided Compute Software will only implement measures such as contacting Data Subjects or notifying the relevant regulator on the instruction of Customer), including, where appropriate, measures to mitigate its possible adverse effects. Where, but only to the extent that it is not possible to provide such information at the same time as the notification of the Personal Data Breach, the information may be provided at a later time but in event as soon as reasonably practicable, and in any event, in sufficient time to enable Customer to meet the applicable deadlines under Applicable Data Protection Laws.

6. Return/Destruction of Personal Data

6.1 In addition to and without prejudice to any obligations set forth in the confidentiality section of these terms or the Agreement, at Customer direction and to the extent feasible Compute Software shall delete or return all Personal Data to Customer at the end of the provision of the applicable Services to which the Processing relates or otherwise upon request, and where and to the extent feasible delete all existing copies held by Compute Software (unless applicable law requires the storage of such Personal Data by Compute Software) and provide confirmation in writing to Customer that it has complied with any such request of Customer.

7. Provide Information as Needed

7.1 Permit Customer to take all necessary steps to ensure compliance under Applicable Data Protection Laws, including, but not limited to, making available to the Customer all information necessary and allowing for audits and inspections if and to the extent necessary to so comply.

7.2 Customer may satisfy any right it may have to conduct an audit or inspection under Article 28 of the GDPR, or under the EU Commission's "Controller-to-Processor Standard Contractual Clauses" (annexed to the EU Commission Decision 2010/87/EU and included as Exhibit C of this DPA), if applicable.

8. Locations and Consent to Sub-processing

8.1 Compute Software shall not subcontract any Processing of Personal Data which Compute Software processes as a Data Processor on behalf of Customer as a Data Controller within the scope of these terms to a third party ("Sub-processor") without Customer's prior consent.

8.2 Customer hereby consents to Compute Software engaging (and/or dismissing) sub-processors to Process the Personal Data provided that: (i) Compute Software provides notice of sub-processors available at <https://www.computesoftware.com/terms>; (ii) Customer may object to the addition of a new Sub-processor appointed by Compute Software if Customer, in its reasonable discretion, believes that such new Sub-processor in Processing the Personal Data would not comply with these terms, the ADPL, or the Agreement, in which case the parties agree to negotiate in good faith a mutually agreeable alternative.

8.3 If the objection is valid and no such alternative is agreed within two months of the objection, Customer will have the right to terminate, without penalty, any Services for which personal data would be Processed by the new Sub-processor against which the objection was raised; (iii) Compute Software shall require by written agreement each Sub-processor's compliance with the ADPL and will ensure it has the contractual terms in place with such Sub-processor that are required by the ADPL; and, (iv) Compute Software shall remain responsible for the Sub-processor's performance under these terms and the Agreement.

8.4 Compute Software will list the locations to which the Personal Data may be transferred in connection with the Service on the aforementioned webpage and shall at all times conduct such transfer in a manner compliant with the ADPL.

9. International Data Exports.

9.1 Data Controller acknowledges that Data Processor and its Sub-processors may maintain data processing operations in countries that are outside of the EEA and Switzerland. As such, Data Processor and its Sub-processors may Process Personal Data in non-EEA and non-Swiss countries. This will apply even where Data Controller has agreed with Data Processor to host Personal Data in the EEA if such non-EEA Processing is necessary to provide support-related or other services requested by Data Controller.

10. Standard Contractual Clauses

10.1 Where Data Processor Processes or permits any Sub-processing entity outside the Processor Group to Process Personal Data in non-EEA countries, Data Processor shall comply with the EU Commission's "Controller-to-Processor Model Clauses" (annexed to EU Commission Decision 2010/87/EU) (the "Clauses") subject to the following provisions:

10.1.1 When used below, the terms "data exporter" and "data importer" shall have the meaning given to them in the Clauses.

10.1.2 Audit of Technical and Organizational Measures. The Parties agree that the audits described in Clauses 5(f) and 12(2) shall be conducted in accordance with the provisions of Section 7 of this DPA.

10.1.3 Sub-processors. Data exporter provides a general consent to data importer, pursuant to Clause 11, to engage onward sub-processors. Such consent is conditional on data importer's compliance with the sub-processing conditions set forth in Section 8 of this DPA. In accordance with the provisions of Clause 5(h), data exporter agrees that new Sub-processors may be appointed by data importer in accordance with the provision of Section 8 of this DPA and acknowledges and accepts that data exporter has the objection rights documented in Section 8 of the DPA.

10.1.4 Obligation of data importer to provide any onward Sub-processor Agreement in accordance with Clause 5(j) to data exporter. The Parties agree that upon the request of data exporter, data importer shall provide all relevant information evidencing compliance with Clause 5(j). Should the information provided by data importer be insufficient to demonstrate data importer's compliance with Clause 5(j) then data importer may provide a version of the onward sub-processor agreement with commercially sensitive and/or confidential information removed. Any such information shall be considered Confidential Information under the confidentiality provisions of the data importer's Services Agreement.

10.1.5 Liability. Pursuant to the provisions of Clause 6, any claims brought under the Clauses shall be subject to the terms and conditions set forth in the Services Agreement. In no event shall any party limit its liability with respect to any Data Subject rights under these Clauses.

10.2 Nothing in the interpretations in this Section 10 is intended to vary or modify the Clauses or conflict with either Party's rights or responsibilities under the Clauses and, in the event of any conflict between the interpretations herein and the Clauses, the Clauses shall prevail to the extent of such conflict.

11. Limitation of Liability

11.1 This DPA shall be subject to the limitations of liability agreed between the Parties (and any reference to the liability of a Party means that Party and its Affiliates in the aggregate). FOR THE AVOIDANCE OF DOUBT, CONTROLLER ACKNOWLEDGES AND AGREES THAT PROCESSOR'S TOTAL LIABILITY FOR ALL CLAIMS FROM CONTROLLER OR ITS AFFILIATES ARISING OUT OF OR RELATED TO THE SERVICES AGREEMENT AND THIS DPA SHALL APPLY IN AGGREGATE FOR ALL CLAIMS UNDER BOTH THE SERVICES AGREEMENT AND THIS DPA. FOR THE AVOIDANCE OF DOUBT, THIS SECTION SHALL NOT BE CONSTRUED AS LIMITING THE LIABILITY OF EITHER PARTY WITH RESPECT TO CLAIMS BROUGHT BY DATA-SUBJECTS.

12. Definitions. For the purposes of this DPA:

12.1. "**Personal Data**", "**Process/Processing**", "**Controller**", "**Processor**", and "**Data Subject**" shall have the same meaning as provided under Applicable Data Protection Laws.

12.2. "**Applicable Data Protection Laws**" or "**ADPL**" means any laws applicable to Compute Software or Customer in relation to the Processing of Personal Data under this Agreement, including: (i) the EU Regulation 2016/679 entitled "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR)" and any applicable national laws made under it; (b) the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded); (c) the Personal Information Protection and Electronic Documents Act of Canada (PIPEDA); and (d) Brazilian Law No. 13,709/2018, as amended (LGPD)

12.3. "**Personal Data Breach**" shall have the meaning set forth in the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016).

EXHIBIT A to DPA
Processing, Personal Data and Data Subjects

1. Data Processor / Data Importer (where applicable):

The Data Processor / Data Importer (where applicable) operates a cloud-based cloud optimization platform. Further information can be found online at www.computesoftware.com.

2. Data Controller / Data Exporter:

The Data Controller /Data Exporter (where applicable) is (please specify briefly your activities relevant to the transfer):

3. Duration of Processing:

The processing of Personal Data shall endure for the duration of the Service Term in the Agreement and this DPA.

4. Data Subjects:

Data Controller / Data Exporter (where applicable) may, at its sole discretion, submit Personal Data to the Service(s), which may include, but is not limited to, the following categories of Data Subjects: employees, relatives of employees, customers, prospective customers, service providers, business partners, vendors, advisors (all of whom are natural persons) of Data Controller / Data Exporter and any natural person(s) authorized by Data Controller / Data Exporter to use the Services.

5. Categories of Personal Data:

Data Controller / Data Exporter (where applicable) may, at its sole discretion, submit Personal Data to the Service(s) which may include, but is not limited to, the following categories of data: first and last name, email address, telephone number, address (business or personal), date of birth, communications (telephone recordings, voicemail), customer service information, title.

6. Special Categories of Data (if appropriate):

7. Processing Operations:

The subject matter of the processing of the personal data:

The Data Processor / Data Importer (where applicable) will host and process personal data in the course of providing its cloud-based cloud optimization platform services to Data Controller / Data Exporter (where applicable).

EXHIBIT B to DPA
Security Standards for Services

Our Sub-Processors, when Processing Personal Data on behalf of Data Controller in connection with the Services, shall implement and maintain the following technical and organizational security measures for the Processing of such Personal Data (“Services Security Standards”):

1. Physical Access Controls: Our Sub-Processors shall take reasonable measures, such as security personnel and secured buildings, to prevent unauthorized persons from gaining physical access to Personal Data, or ensure third parties operating data centers on its behalf are adhering to such controls.

2. System Access Controls: Data Processor shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

3. Data Access Controls: Data Processor shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.

4. Transmission Controls: Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls: Data Process shall take reasonable measures to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed; and, any transfer of Personal Data to a third-party service provider is made via a secure transmission.

6. Data Protection: Reasonable measures are taken to ensure that Personal Data is protected against accidental destruction or loss.

7. Logical Separation: Data from different Data Processor’s subscriber environments is logically segregated on systems managed by the Data Processor to ensure that Personal Data that is collected by different data controllers is segregated from one another.

EXHIBIT C TO DPA
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 organization:
Address:
Email:

(the data **exporter**)

And

Name of the data importing organization: Compute Software, Inc.
Address: 1953 Sage Loop, Mountain View, CA 94043
Email: privacy@computesoftware.com

(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 below.

1. Definitions

For the purposes of the Clauses:

'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;

'the data exporter' means the controller who transfers the personal data;

'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;

'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;

'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;

'technical and organizational 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.

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.

3. Third-party beneficiary clause

3.1 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.

3.2 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.

3.3. 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.

3.4 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.

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 organizational 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; and

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

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 organizational 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.

6. Liability

6.1 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.

6.2 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

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

6.4 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.

7. Mediation and jurisdiction

7.1 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.

7.2 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.

8. Cooperation with supervisory authorities

8.1 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.

8.2 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.

8.3 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).

9. Governing Law

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

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.

11. Sub-processing

11.1 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.

11.2 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.

11.3 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.

11.4 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.

12. Obligation after the termination of personal data processing services

12.1 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.

12.2 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.

Appendix 1 to Exhibit C: the Standard Contractual Clauses

This Appendix forms part of the Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):
Exhibit A of the DPA shall apply.

Data exporter

The data exporter is (please specify briefly activities relevant to the transfer):

Exhibit A of the DPA shall apply.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Exhibit A of the DPA shall apply.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Exhibit A of the DPA shall apply.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Exhibit A of the DPA shall apply.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Exhibit A of the DPA shall apply.

Appendix 2 to Exhibit C: the Standard Contractual Clauses

Data importer (and any sub-processor to data importer) shall implement the technical and organizational measures described in Exhibit B to the Data Processing Addendum executed between data exporter and data importer.

This Appendix forms part of the Clauses.