

## DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) forms a part of the Master Terms found at [www.onespan.com/master-terms](http://www.onespan.com/master-terms), unless Customer has entered into a superseding written master agreement with Supplier, in which case, it forms a part of such written agreement (in either case, the “**Contract**”) between Supplier and Customer for the purchase of internet based services, Support and/or Professional Services from Supplier (identified either as “**Services**” or otherwise in the applicable agreement, and hereinafter defined as “**Services**”).

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 Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term “**Customer**” shall include Customer and Controller Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Contract.

In the course of providing the Services under the Agreement, Supplier may Process certain Personal Data (such terms defined below) on behalf of Customer, and where Supplier Processes such Personal Data on behalf of Customer, the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

### 1. DEFINITIONS

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “**Control**,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“**Controller Affiliate**” means any of Customer's Affiliate(s) (a) that are (i) subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Services pursuant to the Agreement between Customer and Supplier, but have not signed their own Order Form and are not a “**Customer**” as defined under the Agreement, and (b) to the extent Supplier processes Personal Data for which such Affiliate(s) qualify as the Controller.

“**Data Protection Laws**” mean all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates.

“**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/EC (General Data Protection Regulation).

“**Other Controller**” means any entity other than Customer that is Controller of the Customer Personal Data, such as Customer’s affiliated companies or Customer’s client’s, their customers or affiliated companies.

“**Personal Data**” means any Customer Data that relates to an identified or identifiable natural person, which information is subject to the GDPR or the laws of non-EU EEA countries that have formally adopted the GDPR or under any applicable Data Protection Law ; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Personal Data**” also means personal data which Supplier is processing as Processor on behalf of Customer in order to provide the Services. Customer Personal Data includes both, Personal Data controlled by Customer and Personal Data Customer is Processing on behalf of Other Controllers as Processor.

“**Personal Data Breach**” means a suspected or actual 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.

**“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.

**“Processor”** means the entity which Processes Personal Data on behalf of the Controller.

**“Privacy and Security Schedule”** means Supplier’s security and privacy schedule incorporated into the Contract, as updated from time to time, and currently accessible at <https://www.onespan.com/privacy-and-security-terms>.

**“Supplier”** means the Supplier entity which is a party to the Contract.

**“Supplier Group”** means Supplier and its Affiliates engaged in the Processing of Personal Data.

**“Standard Contractual Clauses”** mean the agreement executed by and between Customer and Supplier and attached hereto as Exhibit C (Standard Contractual Clauses) pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

**“Sub-processor”** means any entity engaged by Supplier or a member of the Supplier Group that Processes Personal Data in connection with the Services.

**“Supervisory Authority”** means an independent public authority which is established by an EU Member State pursuant to the GDPR.

## 2. PROCESSING OF PERSONAL DATA

**2.1 Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Supplier is the Processor and that Supplier or members of the Supplier Group will engage Sub-processors pursuant to the requirements set forth in Section 4 “Sub-processors” below.

**2.2 Customer’s Processing of Personal Data.** Customer shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

**2.3 Supplier’s Processing of Personal Data.** As Customer’s Processor, Supplier shall only Process Personal Data for the following purposes: (i) Processing in accordance with the Contract and applicable Order Documents; (ii) Processing initiated by Users and Participants in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Contract (individually and collectively, the **“Purpose”**). Supplier acts on behalf of and on the instructions of Customer in carrying out the Purpose.

**2.4 Details of the Processing.** The subject-matter of Processing of Personal Data by Supplier is as described in the Purpose in Section 2.3. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibit B (Description of Processing Activities) to this DPA.

## 3. RIGHTS OF DATA SUBJECTS

**3.1 Data Subject Requests.** Supplier shall, to the extent legally permitted, promptly notify Customer if Supplier receives any requests from a Data Subject to exercise the following Data Subject rights in relation to Personal Data: access, rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a **“Data Subject Request”**). Taking into account the nature of the Processing, Supplier shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under applicable Data Protection Laws. In addition, to the

extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Supplier shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Supplier is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Supplier's provision of such assistance, including any fees associated with provision of additional functionality.

#### 4. SUB-PROCESSORS

**4.1 Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Supplier's Affiliates may be retained as Sub-processors through written agreement with Supplier and (b) Supplier and Supplier's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. As a condition to permitting a third-party Sub-processor to Process Personal Data, Supplier or a Supplier Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. If applicable, Customer agrees to enter into the Standard Contractual Clauses set out in Exhibit C (Standard Contractual Clauses) and acknowledges that Sub-processors may be appointed by Supplier in accordance with Clause 11 of Exhibit C (Standard Contractual Clauses).

**4.2 List of Current Sub-processors and Notification of New Sub-processors.** A current list of Sub-processors for the Services, including the identities of those Sub-processors is accessible via [https://www.esignlive.com/landings/sub-processors-eu, for OneSpan Sign and via \(link\) for other OneSpan Services](https://www.esignlive.com/landings/sub-processors-eu, for OneSpan Sign and via (link) for other OneSpan Services) ("**Sub-processor Lists**"). Supplier shall provide the Customer with notification of new Sub-processor(s) via the Sub-processor List before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

**4.3 Objection Right for New Sub-processors.** Customer may reasonably object to Supplier's use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Supplier promptly in writing within ten (10) business days after receipt of Supplier's notice in accordance with the mechanism set out in Section 4.2. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Supplier will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Supplier is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Order Form(s) with respect only to those Services which cannot be provided by Supplier without the use of the objected-to new Sub-processor by providing written notice to Supplier. Supplier will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

**4.4 Liability.** Supplier shall be liable for the acts and omissions of its Sub-processors to the same extent Supplier 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 Contract.

#### 5. SECURITY

**5.1 Controls for the Protection of Personal Data.** Supplier shall maintain appropriate technical and organizational measures for 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 the Privacy and Security Schedule. Supplier regularly monitors compliance with these measures. Supplier will not materially decrease the overall security of the Services during a subscription term.

**5.2 Third-Party Certifications and Audits.** Supplier has obtained the third-party certifications and audits

set forth in the applicable Privacy and Security Schedule. Upon Customer's request, and subject to the confidentiality obligations set forth in the Contract, Supplier shall make available to Customer (or Customer's independent, third-party auditor) information regarding the Supplier Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Privacy and Security Schedule. Customer may contact Supplier in accordance with the "Notices" Section of the Contract to request an on-site audit of Supplier's procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Law. Customer shall reimburse Supplier for any time expended for any such on-site audit at the Supplier Group's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Supplier shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Supplier. Customer shall promptly notify Supplier with information regarding any non-compliance discovered during the course of an audit, and Supplier shall use commercially reasonable efforts to address any confirmed non-compliance.

## **6. PERSONAL DATA INCIDENT MANAGEMENT AND PERSONAL DATA BREACH NOTIFICATION**

Supplier maintains security incident management policies and procedures specified in the Privacy and Security Schedule. Supplier shall notify Customer without undue delay of any Personal Data Breach of which Supplier becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under applicable Data Protection Law or which Supplier is required to notify to Customer under applicable Data Protection Law. Supplier shall provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Breach and take commercially reasonable steps to remediate the cause to the extent the remediation is within Supplier's control. Except as required by applicable Data Protection Law, the obligations herein shall not apply to incidents that are caused by Customer, Authorized Users and/or any Non-Supplier Products.

## **7. RETURN AND DELETION OF PERSONAL DATA**

Upon termination of the Services for which Supplier is Processing Personal Data, Supplier shall, upon Customer's request, and subject to the limitations described in the Contract (including the Privacy and Security Schedule), return, or allow Customer to retrieve, all Personal Data in Supplier's possession to Customer or securely destroy such Personal Data and demonstrate to the satisfaction of Customer that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data.

## **8. CONTROLLER AFFILIATES**

**8.1 Contractual Relationship.** The parties acknowledge and agree that, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between Supplier and each such Controller Affiliate subject to the provisions of the Contract and this Section 8 and Section 9. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Contract. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Contract and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Contract and any violation of the terms and conditions of the Contract by a Controller Affiliate shall be deemed a violation by Customer.

**8.2 Communication.** The Customer that is the contracting party to the Contract shall remain responsible for coordinating all communication with Supplier under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

**8.3 Rights of Controller Affiliates.** If a Controller Affiliate becomes a party to the Contract with Supplier, it automatically becomes a party to the DPA with Supplier. In such case Controller Affiliate shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

**8.3.1** Except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against Supplier directly by itself, the parties agree that: (i) solely the Customer that is the contracting party to the Contract shall exercise any such right or seek any such remedy on behalf of

the Controller Affiliate, and (ii) the Customer that is the contracting party to the Contract shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together (as set forth, for example, in Section 8.3.2, below).

**8.3.2** The parties agree that the Customer that is the contracting party to the Contract shall, if carrying out an on-site audit of the Supplier procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Supplier by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Controller Affiliates in one single audit.

## **9. LIMITATION OF LIABILITY**

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Controller Affiliates and Supplier, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Contract, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Contract and all DPAs together.

For the avoidance of doubt, Supplier's and its Affiliates' total liability for all claims from the Customer and all of its Controller Affiliates arising out of or related to the Contract and each DPA shall apply in the aggregate for all claims under both the Contract and all DPAs established under the Contract, including by Customer and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Controller Affiliate that is a contractual party to any such DPA.

## **10. EUROPEAN SPECIFIC PROVISIONS**

**10.1 GDPR.** Supplier will Process Personal Data in accordance with the GDPR requirements directly applicable to Supplier's provisioning of the Services.

**10.2 Data Protection Impact Assessment.** Upon Customer's request, Supplier shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Supplier. Supplier shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority, to the extent required under the GDPR.

**10.3 Transfer Mechanisms.** For transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such applicable Data Protection Law, the Standard Contractual Clauses set forth in Exhibit C (Standard Contractual Clauses) to this DPA apply, subject to Exhibit A (Additional Data Transfer Terms).

**11. Order of Precedence.** Notwithstanding anything to the contrary in the other portions of the Contract, this DPA shall take precedence over conflicting terms in the Contract.

### **List of Exhibits**

**Exhibit A:** Additional Data Transfer Terms

**Exhibit B:** Description of Processing Activities

**Exhibit C:** Standard Contractual Clauses

## EXHIBIT A ADDITIONAL DATA TRANSFER TERMS

### 1. ADDITIONAL TERMS TO STANDARD CONTRACTUAL CLAUSES

**1.1. Customers covered by the Standard Contractual Clauses.** The Standard Contractual Clauses and the additional terms specified in this Exhibit A apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Controller Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Services. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed “data exporters”.

**1.2. Instructions.** This DPA and the Contract are Customer’s complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Contract and applicable Order Document(s); (b) Processing initiated by Users and Participants in their use of the Services; and (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) where such instructions are consistent with the terms of the Contract.

**1.3. Appointment of new Sub-processors and List of current Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) Supplier’s Affiliates may be retained as Sub-processors; and (b) Supplier and Supplier’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Supplier shall make available to Customer the current list of Sub-processors in accordance with Section 4.2 of this DPA.

**1.4. Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Supplier may engage new Sub-processors as described in Sections 4.2 and 4.3 of the DPA.

**1.5. Copies of Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be provided by Supplier to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Supplier beforehand; and, that such copies will be provided by Supplier, in a manner to be determined in its discretion, only upon request by Customer.

**1.6. Audits and Certifications.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Upon Customer’s request, and subject to the confidentiality obligations set forth in the Contract, Supplier shall make available to Customer (or Customer’s independent, third-party auditor) information regarding the Supplier Group’s compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Privacy and Security Schedule. Customer may contact Supplier in accordance with the “Notices” Section of the Contract to request an on-site audit of Supplier’s procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Law. Customer shall reimburse Supplier for any time expended for any such on-site audit at the Supplier Group’s then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Supplier shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Supplier. Customer shall promptly notify Supplier with information regarding any non-compliance discovered during the course of an audit, and Supplier shall use commercially reasonable efforts to address any confirmed non-compliance.

**1.7. Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Supplier to Customer only upon Customer’s request.

**1.8. Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its

Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Exhibit C, the Standard Contractual Clauses shall prevail.

**EXHIBIT B**  
**DESCRIPTION OF PROCESSING ACTIVITIES**

**Data subjects**

Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Users;
- Participants;
- employees of Customer;
- consultants of Customer;
- contractors of Customer;
- agents of Customer; and/or
- third parties with which Customer conducts business.

**Categories of Data**

The Personal Data transferred concern the following categories of Data:

- Any Personal Data comprised in Data, as defined in the Contract.

**Special categories of Data**

Customer may submit Personal Data to Supplier through the Services, the extent of which is determined and controlled by Customer in compliance with applicable Data Protection Law and which may concern the following special categories of data, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic or biometric data;
- health; and
- sex life.

**Processing operations**

The Personal Data transferred will be processed in accordance with the Contract and any Order Document(s) and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain, and update the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Contract, as compelled by law.

**Retention period:** Reference is made to the Privacy and Security Schedule

**Technical and Organizational Measures:** Reference is made to the Privacy and Security Schedule

**Data Protection Officer/Personal Data Breach Reporting:** Reference is made to the Privacy and Security Schedule



## EXHIBIT C

### 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:** **The Customer indicated on the applicable Order Document.**

**Address:** as indicated on the applicable Order Document

**Tel/Fax/email.:** as indicated on the applicable Order Document

(the data **exporter**)

And

**Name of the data importing organization:** The Supplier listed on the applicable Order Document

**Address:** the address listed on the applicable Order Document

**Tel/Fax/email.:** as indicated on the applicable Order Document; [legal@onespan.com](mailto:legal@onespan.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.

#### 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*' mean 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 or 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.

## **Appendix 1 to the Standard Contractual Clauses**

### **Data Exporter**

The Data Exporter is a customer of the Data Importer's communication and productivity software, services, systems and/or technologies.

### **Data Importer**

The Data Importer is a provider of communication and productivity software, services, systems and/or technologies.

### **Data subjects**

Data Exporter may submit personal data to the Data Importer through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Law and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Authorized Users;
- employees of the Data Exporter;
- consultants of the Data Exporter;
- contractors of the Data Exporter;
- agents of the Data Exporter; and/or
- third parties with which the Data Exporter conducts business.

### **Categories of data**

The personal data transferred concern the following categories of data:

Any personal data comprised in Customer Data. "Customer Data" means all data and information submitted by Authorized Users to the Services and includes message text, files, comments and links, but does not include Non-Supplier Products or the Services.

### **Special categories of data**

Data Exporter may submit personal data to the Data Importer through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with Applicable Data Protection Law and which may concern the following special categories of data, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic or biometric data;
- health; and
- sex life.

**Processing operations**

The personal data transferred will be processed in accordance with the Contract and any Order Form and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and update the Services provided to the Data Exporter;
- to provide customer and technical support to the Data Exporter; and
- disclosures in accordance with the Contract, as compelled by law.



## **Appendix 2 to the Standard Contractual Clauses**

Technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

The Data Importer has implemented and will maintain appropriate technical and organizational measures to protect the personal data against misuse and accidental loss or destruction as set forth in Supplier's Privacy and Security Schedule.