DATA PROCESSING ADDENDUM
CONTROLLER-PROCESSOR

This Data Processing Addendum ("**DPA**") forms a part of the Master Terms found at www.onespan.com/master-terms, unless Customer has executed a superseding written 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 Products, Support and/or Professional Services from Supplier (identified either as **"Services"** or otherwise in the applicable agreement, and hereinafter defined as **"Services"**). All capitalized terms not defined herein shall have the meaning set forth in the Contract.

Customer as Controller enters 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. In the course of providing the Services under the Contract, Supplier may Process certain Personal Data on behalf of Customer in compliance with the terms and conditions in this DPA.

HOW TO EXECUTE THIS DPA

This DPA consists of two parts: the main body of the DPA and the Exhibits and Appendices. To enable the quick execution of this DPA, Supplier has pre-signed this DPA and any modifications to this DPA will render the DPA and Supplier's signature null and void.

This DPA has been pre-signed by Supplier, and the particular entity you have purchased from under the applicable Contract shall be deemed the applicable Supplier party under this DPA. Other Supplier entities which may be listed in the signature block are excluded as parties to this DPA.

Signature of the DPA on page 7 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses and its Appendices if applicable to Customer's jurisdiction.

1. To complete this DPA, Customer must:
a) Complete the information in the signature box and sign on Page 7.
b) Send the signed DPA to Supplier by email to DPA@onespan.com

Upon Supplier's receipt of the validly completed DPA, this DPA will become legally binding.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Contract, this DPA is not valid and is not legally binding. Only the Customer entity who is a party to the Contract should execute this DPA.

The provisions of this DPA which relate to the rights of the Customer shall apply to Customer if and to the extent foreseen in the Data Protection Laws applicable to the Processing instruction given by Customer.
The provisions of this DPA which relate to the obligations of the Supplier shall apply to Supplier if and to the extent foreseen in the Data Protection Laws applicable to the Processing instruction given to Supplier.

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. Supplier Affiliates are the legal entities published on the Privacy Center at https://www.onespan.com/privacy-center.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et seq., and its implementing regulations.

"**Controller**" refers to the Customer who 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 and (ii) permitted to use the Services pursuant to the Contract between Customer and Supplier but have not signed their own Order Form and are not a "Customer" as defined under the Contract, and (b) to the extent Supplier processes Personal Data for which such Affiliate(s) qualify as the Controller.

"Data Protection Laws" mean 1) the U.S. Data Protection Laws, 2) the GDPR and the laws of non-EU EEA countries that have formally adopted the GDPR, 3) the Brazilian Data Protection Law (LGPD), Lei Geral de Proteção de Dados Pessoais, (As amended by Law No. 13,853/2019), the Australian Privacy Act 1988 (Cth), or 5) under any other data protection laws applicable to Supplier's Processing of Personal Data hereunder.

"Data Subject" means the Identifiable Natural Person to whom Personal Data relates.

"**General Data Protection Regulation" or "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 regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Identifiable Natural Person" means 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.

"**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, their customers or affiliated companies.

"Personal Data" means any information relating to an identified or Identifiable Natural Person which is Customer Data and that is subject to applicable Data Protection Law. Personal Data includes Personal Data which Supplier is processing as Processor on behalf of Customer 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 breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

"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.

"Product Privacy Statement" means the privacy statement regarding the processing done by Supplier as a processor when providing Products to the Customer. The Product Privacy Statement is published and regularly updated via the Privacy Center.

"**Privacy Center**" means Supplier's privacy center found at https://www.onespan.com/privacy-center. The Privacy Center contains all information about Supplier's processing of Personal Data as a processor, the Product Privacy Statement, the list of sub processors per product or service and issues notifications in case of changes in sub processors.

"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.

"Sensitive Data" means data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Special Categories of Personal Data" means personal data about criminal allegations, proceedings or convictions and information relating to criminal offenses.

"Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

"Supplier" means the OneSpan 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" or "SCC" mean the agreement attached hereto as Exhibit C (Standard Contractual Clauses) subject to Exhibit A (Additional Data Transfer Terms) 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 and the COMMISSION IMPLEMENTING DECISION dated 4 June 2021 Brussels, 4.6.2021, C(2021) 3972 final ANNEX, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"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 1) an EU Member State pursuant to the GDPR or, 2) any other country as per the applicable Data Protection Laws.

"U.S. Data Protection Laws" means all laws and regulations of the United States of America, including the CCPA, applicable to the processing of Personal Data under the Agreement.

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.

2.2.1 Instructions. Customer shall give Personal Data Processing instructions to Processor as agreed by the Parties in the Contract. For the avoidance doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws.

2.2.2 Information Duty. Customer shall process Personal Data in its use of the Service i) in accordance with the requirements of applicable Data Protection Law, and ii) consistent with its instructions to Processor as per clause 2.2.1 above. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data. Customer shall ensure that it has obtained any and all authorizations and lawful bases for Processing Personal Data (including verifiable consent where necessary) in accordance with applicable Data Protection Law Customer acknowledges that the Services can be used for the Processing of Sensitive Data or Special Categories of Personal Data, and Customer agrees not to process any Sensitive Data or Special Categories of Personal Data through the Services unless it has a legal basis and/or authorization to do so in accordance with applicable Data Protection Law. If Customer becomes aware of any breaches of, or other irregularities with, the requirements of applicable Data Protection Laws, , Customer shall promptly notify and provide Processor with instructions detailing the Processing activities Processor must take to ensure the protection of Personal Data, or avoid non-compliance with applicable Data Protection Laws.

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; (ii) Processing initiated by Users 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, duration, nature and purpose of the Processing, and 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.

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"). Considering the nature of the Processing and as far as provided for in applicable Data Protection Laws, 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. 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 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 OneSpan's Privacy Center ("**Sub-processor List**"). Supplier shall update the Sub-processor List before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services. Customer undertakes to subscribe to the ProcessorNotification@onespan.com email so that updates and notifications are automatically received by Customer. Customer is responsible to internally manage such updates and notifications in the light of its rights and obligations under this clause 4.

4.3 Objection Right for New Sub-processors. To the extent provided by applicable Data Privacy Law, 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. 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, Supplier has implemented and maintains technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk of the respective Supplier Service. 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 audit of Supplier's procedures relevant to the protection of Personal Data, but only to the extent specifically required under applicable Data Protection Law. On-site audits are excluded unless specifically required pursuant to mandatory regulations in Customer's jurisdiction. Customer shall reimburse Supplier for any time expended for any such audit at the Supplier Group's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such 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, considering the resources expended by Supplier. Customer shall promptly notify Supplier with information regarding any non-compliance discovered during 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 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. Personal Data incident will not include unsuccessful attempts to, or activities that do not, compromise the security, availability, confidentiality and integrity of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems. 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 Product Privacy Statement and 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. GDPR 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.** Supplier, Supplier Group and its Sub-processors shall process Personal Data in accordance with this DPA outside the EU, in which the Customer is located, including countries where the data protection regulations may not be as stringent in the country of Customer's domicile or registered address or the EEA, Switzerland or UK.
Supplier, Supplier Group and its Sub-processors, as applicable, shall process Personal Data outside of the EU, EEA, Switzerland or UK as permitted under the Data Protection Laws as follows:

(i) where it is determined by the European Union that the destination of the transfer is deemed to have an adequate level of data protection under Art. 45 GDPR; or
(ii) where the Personal Data of Customer is processed in a third country pursuant to adequate safeguards under Art. 46 GDPR including, but not limited to the adoption of Standard Contractual Clauses or an approved code of conduct or an approved certification mechanism. By way of example only, when Supplier uses SCC as safeguard, Supplier has entered the Standard Contractual Clauses prior to the Sub-processor's processing of Personal Data. Customer hereby (for itself as well as on behalf of each Controller Affiliate established within the EEA, UK or Switzerland) accedes to the SCC between Supplier and the Sub-processor.

10.4. **Alternative transfer mechanism**.
To the extent Supplier adopts an alternative data export mechanism (including any new version of or successor to the SCCs) for the transfer of EU Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable EU Data Protection Law and extends to the countries to which EU Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data (within the meaning of applicable EU Data Protection Law), Supplier may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of EU Personal Data.

11. U.S. SPECIFIC PROVISIONS

11. 1. **Relationship**. The parties acknowledge and agree that Supplier is a Service Provider and receives Personal Data pursuant to the business purpose of providing the Services to Customer in accordance with the Contract.

11.2. **Disclosure**. Supplier shall not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the Services, including retaining, using or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Supplier. Supplier certifies that Supplier understands the restrictions in this Section 11 and will comply with them in accordance with the requirements of applicable U.S. Data Protection Laws.

12. GENERAL DATA TRANSFER CONSENT

To the extent that Supplier processes Personal Data protected by an applicable Data Protection Law, the parties acknowledge and agree that Supplier may transfer such Personal Data outside of the territory to which such Data Protection Law Applies subject to Supplier complying with this DPA and the applicable Data Protection Law.

13. **Non-Standard Assistance.** If Customer instructs Supplier to provide assistance relating to the erasure, additional storage, retention of

Customer's Personal Data, or compliance with excessive Data Subject access request received by Customer, then considering relevant factors such as volume of requests, complexity of instructions and timescale requested, Supplier may charge Customer a fee for such non-standard assistance. Such fees shall be assessed in accordance with Supplier's then current Professional Services fees.

14. 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 Clause

The parties' authorized signatories have duly executed this DPA and the attached Exhibits (to the extent such Exhibits are applicable to Customer):

Customer

Customer Legal Name: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____

OneSpan International GmbH

Signature: _____

Name: _____

Title: _____

Date: _____

OneSpan North America Inc.

Signature: _____

Name_____

Title: _____

Date: _____

OneSpan NV

Signature: _____

Name: _____

Title: _____

Date: _____

OneSpan Technology Limited

Signature: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A ADDITIONAL DATA TRANSFER 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 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; (b) Processing initiated by Users 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 9 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 9 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 9 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 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the provisions of clause 5.2 of the DPA.

1.7. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 16.d 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, inconsistency, between the body of this DPA and/or any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Exhibit C or in case of invalid or illegal amendment to the Standard Contractual Clauses made by this DPA and/or any of its Schedules, the Standard Contractual Clauses shall prevail.

EXHIBIT B
DESCRIPTION OF PROCESSING ACTIVITIES

1. Subject matter

The Processing of Personal Data by the Supplier is performed to provide the Services to Customer pursuant to the Contract and are described in the underlying Contract.

Details in terms of the nature and purpose of the Processing are further specified below.

2. **Data Subjects**

Customer may submit Personal Data to the Services, which is determined and controlled by Customer and which may include, but is not limited to, Personal Data relating to the following categories of Personal Data:

☒	Employees (incl. applicants, trainees, former employees) of Customer
☒	Customers of Customer
☒	Employees of customers of Customer
☒	Users of the Supplier Services as contracted by Customer
☒	Agents of Customer
☒	Contractors or Consultants of Customer
☒	Third Parties with which Customer has a business relationship
☒	Participants

3. Categories of Data

Customer determines the Personal Data processed through the Services.
The Personal Data transferred by Customer may concern the following categories of Data:

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

4. **Types of Data**

The Personal Data Processed may concern for example the following types of Data of the above Data Subjects.

☒	Personal master data (customer-number, customer ID or national number or similar)
☒	Name, title, name suffix
☒	Personal telephone number, mobile phone number, e-mail address, fax number ☒business ☒private
☒	Personal address ☒business ☒private
☒	Date of birth/age
☒	Written correspondence or documentation (contract, offers, letters, faxes, messages, e-mails)
☒	Contractual data (contractual relationship with an individual person; an individual's interest in a product or contract)
☒	Contract billing and payment data of an individual person
☒	Customer history of an individual person
☒	Personal data that fall in the category of "professional secret "/professional obligation to discretion (e.g. lawyers, doctors, workers council, data protection officers)
☒	Data relating to criminal activities, misdemeanors or offences of individual persons or the suspicion of such behavior
☒	Data about bank or credit card accounts of individual persons
☒	Financial data of individual persons
☒	Scoring data relating to individuals (e.g., obtained from scoring agencies)
☒	Photographs (identifiable persons)
☒	Data which allows the creation of a personal profile or tracking user behavior (e.g., Tracking Cookies, browsing history)

5. Sensitive Personal Data/Special categories of Personal 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, if any:

☒	Special categories of personal data, i.e., information on one or more of the following ☒racial or ethnic origin, ☒political opinions, ☒religious or philosophical beliefs, ☒trade-union membership, ☒sex life or sexual orientation, ☒health data, ☒genetic data, ☒biometric data

6. Nature and purpose of the Processing

Nature and purpose of the Processing of the Personal Data by the Processor on behalf of the Controller are described precisely and in detail in the underlying Contract and/or the Order that is mentioned within the definition of the Services and referred to here.

The Personal Data may be subject to the following processing activities:

- storage
- processing necessary to provide and update the Services provided to Customer.
- product/service maintenance
- product/service development
- IT management of the systems via which the Services are provide to Customer.
- technical support to Customer; and
- disclosures in accordance with the Contract, as compelled by law.

For the purposes hereof,

- support includes activities related to providing technical support by email or phone; creation of reports; response, analysis, and resolution services; product and service assistance.
- IT management includes activities related to managing the operability, availability and security of a particular product, service, or IT system. This may include incident-tracking, analysis and troubleshooting services.
- Product/services maintenance and development include activities related to product and service maintenance and troubleshooting (e.g., bug fixing) as well as product and services management and development (e.g. new product features or versions).

7. Duration: The duration of the Processing corresponds to the duration of the underlying Contract or the respective Order Document for the Services.

8. Retention period: Subject to Section 7 of the DPA, OneSpan will process Personal Data for the duration of the Contract, unless otherwise agreed upon in writing.

9. **Technical and Organizational Measures:** Technical and Organizational Measures are described in the Privacy and Security Schedule

10. **Data Protection Officer/Personal Data Breach Reporting:** The points of contact are provided for in the Privacy and Security Schedule and the OneSpan Privacy Center at https://www.onespan.com/privacy-center.

11. **List of authorized sub-processors used by Supplier in the provisions of the Services:** The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.

12. Place of Performance: The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.

13. Location of the data centers used by Processor: The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.

14. Transfer of Personal Data: The Personal Data transferred will be transferred to Sub-processors processing activities: The processing of the Personal Data by Data Importer shall be to enable: (1) the performance of the Services; (2) to provide any technical and customer support, maintenance, troubleshooting and IT management as requested by Customer, and (3) to fulfil all other obligations under the Contract.

EXHIBIT C

EUROPEAN COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.
b. The Parties:
   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

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

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);

viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4
Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7 - Optional
Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

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

Clause 9
Use of sub-processors

MODULE TWO: Transfer controller to processor

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

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c. The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.
e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

MODULE TWO: Transfer controller to processor

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

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

MODULE TWO: Transfer controller to processor

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.
d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

MODULE TWO: Transfer controller to processor

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

MODULE TWO: Transfer controller to processor

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

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
    i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
    ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[12];
    iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation

- . The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by

- the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right

to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

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

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   ii. the data importer is in substantial or persistent breach of these Clauses; or
   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

- In these cases, it shall inform the competent supervisory authority

- of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data

importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17
Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b. The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.
c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
d. The Parties agree to submit themselves to the jurisdiction of such courts.

_____

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

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.

Role: Controller

Contact person's name, position and contact details: as indicated on the applicable Order Document.
Role: Controller

Activities relevant to the data transferred under these Clauses: usage of OneSpan SaaS Services as per the 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
Role: Processor
Contact person's name, position and contact details: as indicated on the applicable Order Document.
Role: Controller

Activities relevant to the data transferred under these Clauses: Delivery of OneSpan SaaS Services as per the Order Document

Tel/Fax/email.: as indicated on the applicable Order Document; privacy@onespan.com

(the data **importer**)

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

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

1. **Data Exporter**

The Data Exporter is a customer of the Data Importer's SaaS Services as described in the applicable Order Document.

2. Data Importer

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

3. Subject matter

The subject matter of the Processing under these SCC is described in EXHIBIT B- DESCRIPTION OF PROCESSING ACTIVITIES

4. Data subjects

See EXHIBIT B- DESCRIPTION OF PROCESSING ACTIVITIES

5. Type of data

See EXHIBIT B- DESCRIPTION OF PROCESSING ACTIVITIES

6. Categories of data

See EXHIBIT B- DESCRIPTION OF PROCESSING ACTIVITIES

7. Special categories of data

See EXHIBIT B- DESCRIPTION OF PROCESSING ACTIVITIES

8. Processing operations

See EXHIBIT B- DESCRIPTION OF PROCESSING ACTIVITIES

9. Duration: The duration of the Processing corresponds to the duration of the underlying Contract or the respective Order Document for the Services.

10. **Retention period:** Subject to Section 7 of the DPA, OneSpan will process Personal Data for the duration of the Contract, unless otherwise agreed upon in writing.

11. **Technical and Organizational Measures:** Technical and Organizational Measures are described in the Privacy and Security Schedule

12. **Data Protection Officer/Personal Data Breach Reporting:** The points of contact are provided for in the Privacy and Security Schedule and the OneSpan Privacy Center at https://www.onespan.com/privacy-center.

13. **List of authorized sub-processors used by Supplier in the provisions of the Services:** The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.

14. **Place of Performance:** The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.

15. **Location of the data centers used by Processor:** The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.

16. Transfer of Personal Data: The Personal Data transferred will be transferred to Sub-processors processing activities: The processing of the Personal Data by Data Importer shall be to enable: (1) the performance of the Services; (2) to provide any technical and customer support, maintenance, troubleshooting and IT management as requested by Customer, and (3) to fulfil all other obligations under the Contract.

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.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Belgium

Autorité de la protection des données – Gegevensbeschermingsautoriteit (APD-GBA), https://www.gegevensbeschermingsautoriteit.be/

Rue de la Presse 35 / Drukpersstraat 35

1000 Bruxelles / 1000 Brussel

Drukpersstraat 35, 1000 Brussel

+32 (0)2 274 48 00

+32 (0)2 274 48 35

contact@apd-gba.be

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

The technical and organisational measures are described in OneSpan's Privacy and Security Schedule.

They include the following measures:

- *Measures of pseudonymisation and encryption of personal data*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*
- *Measures for user identification and authorisation*
- *Measures for the protection of data during transmission*
- *Measures for the protection of data during storage*
- *Measures for ensuring physical security of locations at which personal data are processed*
- *Measures for ensuring events logging*
- *Measures for ensuring system configuration, including default configuration*
- *Measures for internal IT and IT security governance and management*
- *Measures for certification/assurance of processes and products*
- *Measures for ensuring data minimisation*
- *Measures for ensuring data quality*
- *Measures for ensuring limited data retention*
- *Measures for ensuring accountability*
- *Measures for allowing data portability and ensuring erasure*

For transfers to subprocessors, OneSpan has agreed in each data processing agreement with such subprocessors on the specific technical and organisational measures to be taken by each subprocessor to be able to provide assistance to the controller.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The controller has authorised the use of the following sub-processors: The list can be found in the Privacy Center set forth at https://www.onespan.com/privacy-center and is updated there in case of changes.