Data Processing Agreement

European Union General Data Protection Regulation Terms ("GDPR Terms")

These General GDPR Terms describe the conditions under which Citrix Systems, Inc. and its Affiliates ("*Citrix*"), on the one hand, and the Partner, on the other hand, shall comply with data protection laws with respect to any personal data relating to European Union residents obtained by one party (acting as a processor) from the other (acting as a controller) and processed for the purpose(s) contemplated by the Agreement.

Definitions

"*Affiliates*" means any entity that controls, is under common control with, or is controlled by Citrix Systems Inc., where "control" means the ownership, direct or indirect, of a majority of an entity's stock or other interest entitled allowing the owner to direct the affairs of such entity.

"*Agreement*" means the applicable Program Guide and/or the contract in force between Citrix and the Partner.

"*Party*" or "*Parties*" shall mean You and/or Citrix.

"*Personal Data*" shall mean personal data, as that term is defined in Article 4 of the GDPR to which one party is provided access for the purpose contemplated by the Agreement.

"*You*" shall mean the Partner.

Terms used but not defined in these GDPR Terms (e.g., "processing", "controller", "processor", "data subject") shall have the same meaning as set forth in Article 4 of the GDPR.

Article 1. Roles and Scope

1. These GDPR Terms apply to either Party's processing of Personal Data.

2. The purpose of these GDPR terms is to govern the processing of Personal Data by the processor in connection with the performance of the Agreement. For purposes of these GDPR Terms, the Parties agree that you and Citrix are either the Controller or the Processor of such Personal Data, as applicable to the performance of the Agreement. However, You and Citrix agree that when a Party referred to as "Controller" appears to be an actual processor, the other party referred to as "Processor" shall be deemed sub-processor of the actual processor.

Article 2. Scope, type and purpose of the personal data processing

Controller determines the scope of Personal Data to which Controller provides Processor access to perform the Agreement. Accordingly, the collection, processing and/or use of Personal Data may relate to the following categories of data

- Personal information: first name, last name, date of birth,
- Communications data: telephone, email, postal mail
- Other: other personal data to which Controller provides Processor access in connection with the performance of the Agreement.

Controller is responsible for providing Processor access only to such Personal Data as needed for performance of the Agreement.

Article 3. Data Processing

1. Processor shall:

a) process the Personal Data only (i) on documented instructions from Controller, as further specified in the Agreement, or (ii) where required to do so by Union or Member State law to which Processor is subject, in which case Processor shall inform Controller in advance, unless prohibited by law;

b) ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) take all measures required of Processor pursuant to Article 32 of the GDPR; where Citrix acts as Processor, the measures required are described in Exhibit 2 below, "Citrix Services Security Exhibit";

d) respect the conditions referred to in Article 4 for engaging another processor;

e) provide Controller reasonable assistance in the fulfilment of Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

f) assist Controller in ensuring Controller's compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Citrix;

g) return or provide an opportunity for Controller to retrieve all Personal Data after the termination of the Agreement and delete existing copies as follows: Controller shall have thirty (30) calendar days to download its Personal Data after termination of the Agreement and must contact the Processor's technical support for download access and instructions. Should Controller not contact Processor's technical support for this purpose within thirty (30) calendar days after the termination of the Agreement, Processor shall delete Controller Personal Data promptly once that Personal Data is no longer accessible by Controller, except for (i) secure back-ups deleted in the ordinary course, and (ii) retention as required by applicable law; in the event of either (i) or (ii), Processor will continue to comply with the relevant provisions of these GDPR Terms until such data has been deleted;

h) make available to Controller information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits by Controller or Controller third-party auditor, in accordance with Article 10 below;

i) inform Controller if, in Processor's opinion, any instruction infringes the GDPR or other Union or Member State data protection provisions, provided that Processor shall have no obligation to independently inspect or verify Controller use or processing of Personal Data; and

j) inform Controller of and provide Controller reasonable assistance in meeting Controller's obligations in regard to any Personal Data breach, in accordance with Article 8 below.

2. Where Processor engages another processor for carrying out specific processing activities on Controller behalf, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor as applicable by way of a contract, or other legal act under Union or Member State law, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the applicable requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Processor shall remain responsible for the performance of that other processor's obligations.

Article 4. Sub-processing

1. Subject to the terms of this Article 4, Controller consent to Processor engaging Sub-processors for the processing of Personal Data.

2. Processor will ensure that Sub-processors are bound by written agreements that require them to provide at least the level of data protection required of Processor by these GDPR Terms.

3. Processor remains responsible at all times for such processors' compliance with these GDPR Terms as applicable.

4. A list of Processor's current Sub-processors are set forth in the List of Sub-processors made available to Controller. Processor will update the List of Sub-processors and provide Controller with a mechanism to obtain notice of that update promptly upon commissioning a new Sub processor. The following terms shall also apply:

a) If Controller does not approve a new Sub-processor, then Controller may terminate any subscription for the affected service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval.

b) If the affected service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite.

c) After termination, Controller shall remain obligated to make all payments required under any purchase order or other contractual obligation relating to the affected service and shall not be entitled to any refund or return of payment.

Article 5. Onward and International Data Transfer

Where You are the Controller and Citrix is the Processor, the following terms apply:

1. Citrix may transfer Personal Data to the United States and/or to other third countries where Citrix or its processors operate. Citrix will follow the requirements of these GDPR Terms regardless of where such Personal Data is stored or processed.

2. Attached hereto as Exhibit 1 is the "Standard Contractual Clauses ("Processor")" specified in European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of data to processors established in third countries under the European Data Protection Directive. Where You provide Personal Data governed by the General Data Protection Regulation and there is not another legitimate basis for the international transfer of such Personal Data, the "Standard Contractual Clauses - Processor" specified in such Decision shall apply. In such case, Article 1 of Exhibit 2 (Citrix Services Security Exhibit) shall constitute Appendix II to the Standard Contractual Clauses (description of technical and organizational security measures). In the event that such Decision is deemed invalid, the Parties agree to negotiate in a timely way and in good faith any replacement terms as may be required for the international transfer of such Personal Data. For further information concerning audits performed under the Standard Contractual Clauses, see Article 10, Audits, below.

3. In addition, Citrix may process and disclose Personal Data (a) to its Affiliates, for purposes consistent with the Agreement and these GDPR Terms; (b) in connection with any anticipated or actual merger, acquisition, sale, bankruptcy or other reorganization of some or all of its business, subject to the obligation to protect Personal Data consistent with the terms of the Agreement; or (c) for legal purposes, including enforcement of its rights, detecting and preventing fraud, protecting against harm to the rights or property of Citrix, Citrix or Your users, or the public; and (c) as required by law, including in response to a subpoena, judicial or administrative order, or other binding instrument (each a "Demand"). Except where prohibited by law, Citrix will promptly notify You of any Demand and provide You reasonable assistance to facilitate Your timely response to the Demand.

Article 6. Assisting Controller Response to Requests from Data Subjects

1. Processor will make available to Controller the Personal Data of Controller's data subjects and the ability to fulfill requests by data subjects to exercise one or more of their rights under the GDPR. Processor shall comply with reasonable requests to assist with Controller's response.

2. If Processor receives a request from Controller's data subject to exercise one or more of its rights under the GDPR, Processor will redirect the data subject to make its request directly to Controller.

Article 7. Security Terms

Processor and Controller shall maintain security measures and practices for the protection of personal data. To this extent, the Parties agree that:

a) Citrix, when it acts as Processor (and You are the Controller), shall maintain the security measures as set forth in Exhibit 2 "Citrix Services Security Exhibit". Citrix may update the practices specified in Exhibit 2, provided that the measures provided until the term of the Agreement shall in no event provide no less protection than those included as of the term of such Agreement; and

b) Partner, when it acts as Processor (and Citrix is the Controller), shall maintain security measures at least as protective as those specified for Citrix in Exhibit 2 "Citrix Services Security Exhibit".

Article 8. **Personal Data Breach**

Processor shall notify Controller without undue delay after becoming aware of a data breach relating to Personal Data. Such notification shall at least:

a) describe the nature of the Personal Data breach including, where possible, the categories and approximate number of Controller's data subjects concerned and the categories and approximate number of Personal Data records concerned;

b) provide the name and contact details of the data protection officer or other contact where more information can be obtained; and

c) describe the measures taken or proposed to be taken to address the Personal Data breach including, where appropriate, measures to mitigate its possible adverse effects.

Article 9. **Records of Processing Activities**

Processor shall maintain all records of processing activities required by Article 30(2) of the GDPR.

Article 10. **Audit right**

Controller may carry out audits of Processor's processing of Controller's Personal Data as required by law. Any such audit shall be conducted at Controller's own expense, during normal business hours, without material disruption to Processor's business, and in accordance with Processor's security rules and requirements. Prior to any audit, Processor undertakes to provide Controller reasonably requested information and associated evidence to satisfy Controller's audit obligations, and Controller undertakes to review this information prior to undertaking any independent audit.

Controller may use a third-party auditor with Processor's agreement, which shall not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Processor.

Article 11. **Modification, Supplementation, and Term**

1. Each Party may modify or supplement these GDPR Terms, with notice to the other Party, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with applicable law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40 and 42 of the GDPR.

2. Without prejudice to these GDPR Terms, Citrix, when acting as Processor, may from time to time provide additional information and detail about how it will execute these GDPR Terms in its product-specific technical, privacy, or policy documentation.

3. These GDPR Terms become effective upon effectiveness of the GDPR.

For the Partner	For Citrix
Name: …	Name: Antonio Gomes
Function	Function: SVP and General Counsel
Authorised Signature …	Authorised signature…
	Antonio Gomes Antonio Gomes (Mar 16, 2018)

Exhibit 1: Standard Contractual Clauses ("Processor")

EU Commission Standard Contractual clauses for the transfer of personal data to processors established in third countries

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

You

(the data **exporter**)

And

Citrix Systems, Inc., and its Affiliates

Address: 851 West Cypress Road, Ft. Lauderdale, FL 33309

Tel.:+1 954 267 3000; fax: + 1 805 690 6471; e-mail: modelclauses@citrix.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 [(1)];

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer [(2)]

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial

information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor 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 sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

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

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

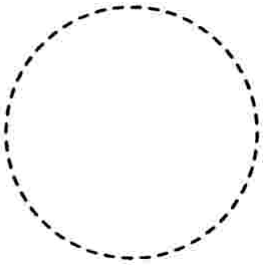
On behalf of the data exporter:

Name (written out in full): …

Position: …

Address: …

Other information necessary in order for the contract to be binding (if any):

	Signature …

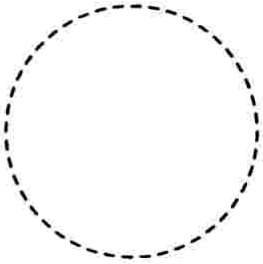
On behalf of the data importer:

Name (written out in full):

Position:

Address: …

Other information necessary in order for the contract to be binding (if any):

	Signature … Antonio Gomes Antonio Gomes (Mar 16, 2018)

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(3) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

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

Data exporter

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

A Citrix partner, marketing and distributing Citrix products and services to other Citrix partners and/or its customers.

Data importer

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

Providing IT products, services and solutions as described in Citrix Services Description.

Data subjects

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

As described in Article 3 of the Data Processing Agreement.

Categories of data

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

As described in Article 3 of the Data Processing Agreement.

Special categories of data (if appropriate)

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

As described in Article 3 of the Data Processing Agreement.

Processing operations

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

As described in the Service Description.

For the Partner	For Citrix
Name: …	Name: Antonio Gomes
Function	Function: SVP and General Counsel
Authorised Signature …	Authorised signature…
	Antonio Gomes Antonio Gomes (Mar 16, 2018)

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Technical and organisational security measures are described in Citrix Services Security Exhibit (Exhibit 2 to the agreement)

For the Partner	For Citrix
Name: …	Name: Antonio Gomes
Function	Function: SVP and General Counsel
Authorised Signature …	Authorised signature…
	Antonio Gomes Antonio Gomes (Mar 16, 2018)

Exhibit 2 - Citrix Services Security Exhibit

This Citrix Services Security Exhibit (the *Exhibit*) describes the technical and organizational security controls employed in connection with Citrix Cloud services, technical support services or consulting services under a Citrix license, subscription or services Agreement (the "*Agreement*"). This Exhibit does not apply to beta or lab/tech preview services, including Citrix Cloud Labs.

Capitalized terms have the meaning stated in the Agreement or as defined herein, including Article 7, Definitions, below.

For clarity, where Partner acts a data Processor, Partner shall implement controls at least as protective as those specified under this Exhibit.

Article 1. Citrix Security Controls

This Article describes the physical, logical and administrative controls Citrix employ to secure the Services and Partner's associated security obligations. Citrix employs ISO/IEC 27002 as the baseline for its Services security program.

The controls specified in Article 1.A apply to all Services. The additional controls specified in Section 1.B apply to all generally available Citrix Cloud Services (collectively "Cloud Services").

Citrix reserves the right to modify the controls specified in this Article 1 provided that the controls employed during a term of service for which Partner has paid shall remain at least as protective of Partner Personal Data as those specified in this Article 1 on the effective date of such term.

1.A. Enterprise Security Controls – All Services

Area	Control(s)
Security Program Management	**Security Ownership**. Citrix has appointed one or more security officers responsible for coordinating and monitoring the security controls for the Services. **Security Roles and Responsibilities**. Citrix personnel with access to Partner Personal Data are subject to confidentiality obligations. **Service Security Policies.** Citrix maintains a comprehensive Global Security Framework (GSF), which provides the overarching security and safety principles established and approved by Citrix executive management. Policies provide security requirements in a clear and concise manner. Standards define the process or methodology of meeting policy requirements. The GSF security program undergoes regular reviews and evaluations. Citrix maintains a summary of the GSF program and will provide it to Partners upon request. **Product Risk Management.** Citrix performs assessments of key areas of risk associated with the Services including, by way of example only and as applicable, privacy risk assessments, open source reviews and export control analysis.
Asset Management	**Asset Inventory**. Citrix maintains an inventory of Citrix-managed equipment used to perform the Services ("Assets"). Identified system owners are responsible for maintaining and updating the inventory as needed.

Area	Control(s)
	Asset and Data Handling Citrix identifies and classifies Partner Personal Data to ensure access is appropriately restricted. Citrix imposes restrictions on printing Partner Personal Data and disposing of printed materials that contain Partner Personal Data. Citrix personnel must obtain authorization prior to storing Partner Personal Data on portable devices, remotely accessing Partner Personal Data, or processing Partner Personal Data outside facilities managed by Citrix or its service providers.
Access Management	**Access Policy.** Citrix maintains a record of security privileges of individuals having access to Partner Personal Data and follows the principle of least-privilege. **Access Authorization** Citrix maintains and updates a record of personnel authorized to access Citrix systems that contain Partner Personal Data. New access to systems is reviewed and approved by management prior to being granted. Citrix performs regular reviews of user accounts and assigned permissions for key systems. Citrix identifies those personnel who may grant, alter or cancel authorized access to data and resources. Citrix ensures that where more than one individual has access to systems containing Partner Personal Data, the individuals have separate identifiers/log-ins. **Least-Privilege** Citrix restricts access to Partner Personal Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** Citrix requires that users secure computers and data while unattended. Citrix requires that passwords remain unintelligible throughout their lifecycle. **Authentication** Citrix uses industry-standard practices to identify and authenticate users accessing information systems. Where authentication mechanisms are based on passwords, Citrix follows industry-standard practices for password handling and management, including: Passwords are renewed regularly, as dictated by system requirements and Citrix standards Passwords must meet length and complexity requirements, including a minimum length of 8 characters Personnel are prohibited from sharing passwords De-activated or expired identifiers are not granted to other individuals Citrix maintains procedures to deactivate passwords that have been corrupted or inadvertently disclosed. Citrix monitors repeated attempts to gain access to the services using an invalid password.

Area	Control(s)
	Citrix uses practices designed to maintain the confidentiality and integrity of passwords when they are assigned, distributed and stored.
Loss Prevention	**Malicious Software**. Citrix uses anti-virus software and other controls to avoid malicious software gaining unauthorized access to Partner Personal Data, including malicious software originating from public networks. **Media Disposal.** Citrix disposes of media when no longer required based on classification and using secure deletion processes.
Physical and Environmental Security (Access Control, Availability Control)	**Physical Access to Citrix Facilities**. Citrix limits facilities access to authorized individuals. ID badges are required for employees, contractors and guests and must be visible at all times when in the facility. Citrix monitors facility entry points using various methods including security guards, intrusion detection and CCTV cameras. **Protection from Disruptions**. Citrix uses systems to protect against loss of data due to power supply failure or line interference, including global and redundant service infrastructure that is set up with disaster recovery sites; evaluating data centers and Internet service providers (ISPs) to optimize performance regarding bandwidth, latency and disaster recovery isolation; situating data centers in secure facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy; and uptime agreements from key suppliers. **Hosted Data Centers.** When Citrix uses third-party co-located data centers for provision of the Services, Citrix requires that the service provider meets or exceeds the physical and environmental security requirements of Citrix-managed facilities. Minimum security requirements include, but are not limited to: • Physical access restrictions and safeguards (authentication, logs, monitoring, etc.) • Adequate separation of environments • Fire suppression, detection, and prevention mechanisms • Climate control systems (temperature, humidity, etc.) **Cloud Computing.** When Citrix uses XaaS [Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)] for provision of the Services, Citrix contracts with XaaS providers that provide a materially similar level of physical access control to its hosted data centers.
Application and Development Security	**System Development & Maintenance.** Citrix maintains a Secure by Design process, which includes standards and change control procedures designed to address security requirements of information systems, code review & testing, and security around the use of test data. This process is managed and monitored

Area	Control(s)
	by a specialized security engineering team, which is also responsible for design review, threat modeling, manual code review & spot checks, and penetration testing. **Open Source Management**. Citrix uses a software-based system for managing open source reviews and approvals. In addition, Citrix conducts periodic scans and audits of its software products to confirm open source compliance. **Change Management.** Citrix maintains change control procedures that address security requirements of information systems, testing, acceptance of testing, and security around the use of test data. Software and configuration changes are managed and tracked using standard ticketing systems.
Secure operations	**Network Design**. Citrix implements mechanisms designed to enforce access management policies and standards across the services, including network controls over access to Partner Personal Data. These include, as appropriate: configuring an intermediate untrusted zone between the Internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic; and separating web and application servers from the corresponding database servers in a tiered structure that restricts traffic between the tiers.
Incident Management	**Incident Response**. Citrix maintains an incident response program designed to contain, analyze, remediate and communicate security and safety incidents impacting Citrix managed networks and/or systems or Partner Personal Data. **Incident Notification**. If Citrix determines that Partner Personal Data within its control has been subject to a Security Incident, Partner will be notified within the time period required by applicable law. **Incident Recording**. Citrix maintains a record of known Security Incidents with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, and the procedure for recovering data and services as applicable.
Vendor Management	**Onboarding**. Citrix performs security assessments of service providers that will have access to Partner Personal Data and/or to components of the Services that process Partner Personal Data. Citrix requires service providers connected with the Services to comply with the level of security in this Section applicable to the services they provide. Service providers that may access Partner Personal Data subject to European Union law are required to self-certify to EU-U.S. and EU-Swiss Privacy Shield programs or to execute Standard Contractual Clauses. **Ongoing Maintenance.** Service providers are assessed periodically, based upon the sensitivity and risk associated with their services.

Area	Control(s)
	Off-boarding. Upon termination of a supplier relationship, the service provider is required to return all Partner Personal Data in its possession or to certify that all Partner Personal Data has been securely destroyed.
Business Continuity and Disaster Recovery	**Business Continuity.** Citrix maintains emergency and contingency plans for the facilities in which Citrix information systems that process Partner Personal Data are located. **Disaster Recovery.** Citrix's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Partner Personal Data in its original or last-replicated state.
Partner Security Obligations	Partner is responsible for managing security not expressly included as part of the Services. This includes, but is not limited to: • Limiting Citrix's access to Partner Personal Data only to what is needed for Partner to receive the Services. • Protecting its network and service components against interference, including monitoring and securing its networks and computing equipment. • Downloading Partner Personal Data where needed, both during the term of Services and upon termination. • Citrix either encrypts data in transit by default or offers Partners means to encrypt data in transit. Further detail is provided in the product documentation for the Services. Partner is responsible for ensuring that data is appropriately secured in transit.

1.B. Additional Cloud Services Security Controls

Area	Control(s)
Data Protection (Availability Control, Transmission Control, Data Deletion)	**Failover Procedures**. Citrix implements mechanisms designed to address loss of availability of Partner Personal Data, including storing copies of Partner Personal Data in a different place from where the primary computer equipment processing the Partner Personal Data is located. **Data Beyond Boundaries**. Citrix encrypts or enables Partner to encrypt Partner Personal Data that is transmitted over public networks that are part of a Service. **Retention.** Citrix may retain Partner Personal Data following the Service period and archiving for Partner access where required for legal purposes. Citrix will comply with the requirements of this Exhibit until such Partner Personal Data has been permanently deleted. Subject to Return directly below, Citrix is under no obligation to retain Partner Personal Data following termination of the Service. **Return.** Subject to availability and the applicable Services Description, Partner has thirty (30) days to download Partner Personal Data after expiration.

Area	Control(s)
	Data Deletion. Citrix will securely delete Partner Personal Data when no longer needed for a legitimate purpose.
Secure operations	**Event Logging**. In certain Services, Citrix collects Logs. Logs may include access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant activity. Logs are used (**i**) for providing, securing, managing, measuring and improving the Services and associated analytics, (**ii**) as directed or instructed by Partner and its Users, and/or (**iii**) for compliance with Citrix policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage and security of the Services and related components. Partner may not block or interfere with this monitoring. Citrix may supplement Logs with information collected from third parties for the purposes specified above. Logs may be used for purposes not specified in this Exhibit only in aggregate form.
Business Continuity and Disaster Recovery	**Back-ups.** Except where otherwise noted in the respective Services Description, Services are maintained in high availability, active-active clusters spanning multiple physical sites. Systems not maintained in an active-active configuration are backed up according to the specific Service's Service Level Goals.

Article 2. Treatment of Personal Data

Personal data is information about an identified or identifiable individual. Partner determines the personal data that it includes in Partner Personal Data. In performing the Services, Citrix acts as a data processor and Partner remains the data controller for any personal data contained in Partner Personal Data. Citrix will act on Partner's instructions regarding the processing of such personal data, as specified in the Agreement.

Further information concerning the treatment of personal data subject to the General Data Protection Regulation, including the mechanisms employed for international transfer of such data, is provided in Exhibit I, General Data Protection Regulation Terms.

Article 3. Location of Services

Partner Personal Data may be transferred to, stored and/or processed in the United States or in other countries where Citrix and/or its service providers operate. The requirements of this Exhibit continue to apply, regardless of where Citrix stores or processes Partner Personal Data.

The parties may negotiate in good faith regarding any further data processing or data transfer agreements needed to facilitate the lawful transfer of data internationally in connection with Citrix's provision of the Services.

Article 4. Disclosure of Partner Personal Data

Partner consents to Citrix's disclosure of Partner Personal Data as set forth in this section.
Citrix may use subcontractors and agents to perform Services. Any subcontractors and agents shall be entitled to access Partner Personal Data only as needed to perform the Services and shall be bound by written agreements that require them to provide at least the level of data protection required of Citrix by this Exhibit, as applicable. Citrix remains responsible at all times for its subcontractors' and agents' compliance with the terms of the Agreement, as applicable.

Citrix also may disclose Partner Personal Data to (a) its Affiliates, for purposes consistent with the Agreement; (b) in connection with any anticipated or actual merger, acquisition, sale, bankruptcy or other reorganization of some or all of its business, subject to the obligation to protect Partner Personal Data consistent with the terms of the Agreement; or (c) for legal purposes, including enforcement of its rights, detecting and preventing fraud, protecting against harm to the rights or property of Citrix, partners, Users, or the public; and (c) as required by law, including in response to a subpoena, judicial or administrative order, or other binding instrument (each a "Demand"). Except where prohibited by law, Citrix will promptly notify Partner of any Demand and provide Partner assistance reasonably necessary for Partner to respond to the Demand in a timely manner.

Article 5. Partner Obligations

1. General. Partner may use and access the Services only as permitted by the Agreement. Partner will comply with all laws applicable to it in connection with its use of the Services.

2. Permissions. Partner is responsible for obtaining all permissions necessary for Citrix to perform the Services, including providing any notices and obtaining any consents or licenses needed for Citrix to access and process the Partner Personal Data as set forth in this Exhibit.

3. Regulatory. Partner is responsible for determining whether any Partner Personal Data is subject to additional regulatory or security requirements beyond those specified in the Agreement, including this Exhibit. Partner shall not submit or store any Partner Personal Data that is governed by US International Traffic in Arms Regulations (ITAR) or similar regulations of any country that restricts import or export of defense articles or defense services. Further, Partner shall not provide or store any Partner Personal Data subject to additional regulatory requirements, such as protected health information ("PHI"), payment card information ("PCI"), or controlled-distribution data under government regulations, unless specified in the Partner's Order and applicable Service Description and the parties have entered into any additional agreements (such as a Business Associate Agreement (BAA)) in advance as may be required for Citrix to process such data. Partners of the ShareFile service may contact Citrix at privacy@sharefile.com to request a BAA.

4. Partner Security Environment. The Services are designed to be delivered only within a larger Partner security environment. Partner shall ensure appropriate security functionality for all components not expressly managed by Citrix including, but not limited to, access controls, firewalls, applications and networks used in conjunction with the Services. See Section 1.A., Partner Security Obligations, above.

5. Security Notification. Partner is responsible for notifying Citrix promptly of any security incidents involving the Services and/or Partner Personal Data.

6. User Compliance. Partner is responsible for its Users' compliance with the terms of the Order and the Agreement.

Article 6. Citrix Contacts

FUNCTION	CONTACT
Partner Support	https://www.citrix.com/contact/technical-support.html
Reporting an Incident	secure@citrix.com

Suspected vulnerabilities in Citrix products	secure@citrix.com

Article 7. Definitions

Capitalized terms in the Exhibit shall have the meaning specified in the Agreement or below. In the event of a conflict between the remaining terms of the Agreement and any definition below, the definition below shall apply to this Exhibit.

Partner Personal Data means any data uploaded to Partner's account for storage or data in Partner's computing environment to which Citrix is provided access in order to perform Services.

Log means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.

Security Incident means unauthorized access to Partner Personal Data resulting in the loss of confidentiality, integrity or availability.

Effective: February 15, 2018