Cloud Software Group

PARTNER DATA PROCESSING ADDENDUM

Version: January 4, 2023

1. Scope, Order of Precedence and Parties

This Partner Data Processing Addendum ("DPA") applies to the Processing of Personal Data by one party acting as a Processor on behalf of the other party acting as a Controller in connection with the relevant Cloud Software Group Program Guide and/or the contract in force between Cloud Software Group ("CS Group") (acting on its own behalf and as agent for each Affiliate) and the Partner (acting on its own behalf and as agent for each Affiliate) ("Partner", "You") (collectively, the "Agreement"). Partner shall at all times remain responsible for the performance of its Affiliates under the Agreement, including this Addendum.

In the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA shall control. In the event of a conflict between the terms of this DPA and the EU Standard Contractual Clauses, the terms of the EU Standard Contractual Clauses shall control.

2. Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly.

"**Adequacy Decision**" means a decision of the European Commission under Applicable Law that a Transfer of Personal Information ensures an adequate level of protection.

"**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with the relevant party.

"**Applicable Data Protection Laws**" means (i) the EU General Data Protection Regulation 2016/679/EU ("GDPR") and laws or regulations implementing or supplementing the GDPR; and (ii) any other international, federal, state, provincial and local privacy or data protection laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective that apply to the Processing of Personal Data under this Agreement.

"**2021 EU Standard Contractual Clauses**" or "**2021 EU SCCs**" mean the contractual clauses annexed to the EU Commission Decision 2021/914/EU or any successor clauses approved by the EU Commission.

"**GDPR**" means EU General Data Protection Regulation 2016/679/EU.

"**Individual**" means any identified or identifiable individual about whom Personal Information may be Processed under the Agreement.

"**International Transfer**" means the access, transfer, delivery, or disclosure of Personal Information to a person, entity or computing system located in a country other than the country from which the Personal Information originated.

"**Personal Data**" means any information Processed in connection with the performance of the Agreement that can identify a unique individual, 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 individuals or as such information may be otherwise defined under Applicable Data Protection Laws.

"**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 transmitted, stored or otherwise Processed in order to perform the Services that compromises the confidentiality, integrity, or availability of the Personal Data.

"**Swiss SCC Addendum**" means adaptation of the 2021 EU SCCs to comply with the Swiss legislation in order to ensure an adequate level of protection for data transfers from Switzerland to a third country subject to the Swiss Federal Act on Data Protection ("**FADP**").

"**UK Data Protection Laws**" means the UK GDPR and the Data Protection Act 2018, or any successor UK data protection laws as updated, amended or replaced from time to time.

"**UK SCC Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (vB1.0 or any subsequent version) issued by the UK Information Commissioner's Office.

Terms used but not defined in this DPA (e.g., "Business Purpose, Consumer, Controller, Data Subject, Process/Processing, Processor, Supervisory Authority") shall have the same meaning as set forth in the Agreement or Applicable Data Protection Laws (except in the context of Module Three of the 2021 EU SCCs when "Controller" as used herein is a Data Exporter acting as a Processor, in which case Processor shall mean Sub-Processor).

3. Roles as Data Controller and Data Processor

For purposes of this DPA, You and CS Group are either both acting as Controllers or one as the Controller and the other as the Processor of the Personal Data, as applicable to the performance of obligations under the Agreement. The Controller is responsible for complying with its obligations as a Controller under Applicable Data Protection Laws governing the provision of Personal Data to the other party under the Agreement, including without limitation obtaining any consents, providing any notices, or otherwise establishing the required legal basis. Unless specified in the Agreement, neither party will provide the other with access to any Personal Data that imposes specific data protection requirements greater than those agreed to in the Agreement and this DPA, and the Controller will limit the other party's access to Personal Data as necessary under the Agreement.

A party acting as a Processor is responsible for complying with its obligations under Applicable Data Protection Laws that apply to its Processing of Personal Data under the Agreement and this DPA.

4. Purpose of Processing

Processor and any persons acting under its authority under this DPA, including sub-Processors and Affiliates as described in Section 6, will Process Personal Data only in accordance with Controller's written instructions as specified in the Agreement, this DPA and in accordance with Applicable Data Protection Laws. Neither party will disclose Personal Data in response to a subpoena, judicial or administrative order, or other binding instrument (a "Demand") unless required by law. Each party will promptly notify the other of any Demand unless prohibited by law and provide the other party reasonable assistance to facilitate a timely response to the Demand.

CS Group may also provide Personal Data to Affiliates 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 this DPA.

5. Data Subjects and Categories of Personal Data

Controller determines the Personal Data to which it provides access to under the Agreement. This may involve the Processing of Personal Data of the following categories of Data Subjects:

- Employees and applicants
- Prospects, customers and end users
- Suppliers, agents and contractors

The Processing of Controller's Personal Data may also include the following categories of Personal Data:

- Direct identifiers such as first name, last name, date of birth, and home address
- Communications data such as home telephone number, cell telephone number, email address, postal mail and fax number
- Family and other personal circumstance information, such as age, date of birth, marital status, spouse or partner, number and names of children
- Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, CV data
- Other data such as financial, good or services purchased, device identifiers, online profiles and behaviour, and IP address
- Other Personal Data to which Controller provides Processor access in connection with the Agreement

6. Sub-Processing

Subject to the terms of this DPA, Controller authorizes the other party when acting as a Processor to engage sub-Processors and Affiliates for the Processing of Personal Data. These sub-Processors and Affiliates are bound by written agreements that require them to provide at least the level of data protection required of Processor by the Agreement and this DPA. Controller may request Processor to perform an audit on a sub-Processor or to obtain an existing third-party audit report related to the sub-Processor's operations to verify compliance with these requirements. Controller may also request copies of the data protection terms Processor has in place with any sub-Processor or Affiliate involved in providing the Services. Processor remains responsible at all times for such sub-Processors' and Affiliates' compliance with the requirements of the Agreement, this DPA and Applicable Data Protection Laws.

Processor shall maintain a list of sub-Processors and Affiliates, as well as a mechanism to obtain notice of any updates to the list. CS Group's list is available at https://www.citrix.com/buy/licensing/subprocessor-list.html. At least fourteen (14) calendar days before authorizing any new sub-Processor to access Personal Data, Processor will update the list of sub-Processors and Affiliates. The following terms also apply:

- If, based on reasonable grounds related to the inability of such sub-Processor or Affiliate to protect Personal Data, Controller does not approve of a new sub-Processor or Affiliate, then it 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.
- If the affected service is part of a suite (or similar single purchase of services), then any such termination will apply to the entire suite.
- After such termination, Controller shall remain obligated to make all payments required under any purchase order or other contractual obligation related to the affected service and shall not be entitled to any refund or return of payment.

7. International Transfer of Personal Data

Processor may transfer Personal Data to the United States and/or to other third countries as necessary under the Agreement, and Controller appoints Processor to perform any such transfer in order to process Personal Data as necessary under the Agreement. Processor will follow the requirements of this DPA regardless of where such Personal Data is stored or Processed.

International Transfers of Personal Information. To the extent that the performance of obligations under the Agreement involve an International Transfer of Personal Information between the parties, the International Transfer shall be subject to the terms of this Addendum. If additional terms are required to meet the requirements for International Transfers from a specific jurisdiction, the Parties agree to negotiate in good faith to amend this Addendum to include the required terms.

International Transfers from the EEA, Switzerland, and UK. To the extent that the performance of obligations under the Agreement involve the International Transfer of Personal Information of a resident(s) of a country within the European Economic Area ("EEA"), Switzerland or United Kingdom ("UK") to the other party located outside of the EEA, Switzerland or UK and the International Transfer is not covered by an Adequacy Decision and there is not another legitimate basis for the international transfer of such Personal Information, then such transfers are subject to either the 2021 EU Standard Contractual Clauses, UK SCC Addendum and/or Swiss SCC Addendum (as applicable) or other valid transfer mechanisms available under Applicable Law. For international transfers subject to:

- the GDPR, the Parties hereby incorporate by reference the 2021 EU SCCs in unmodified form (Module One where both parties are a Controller and/or Module Two where one party is a Controller and the other party is a Processor);
- the UK Data Protection Laws, the Parties hereby incorporate by reference the UK SCC Addendum in unmodified form; and
- The FADP, the Parties hereby incorporate by reference the Swiss SCC Addendum.

With respect to the 2021 EU SCCs, the Parties agree to the following: (i) Clause 7 shall be omitted; (ii) Clause 9 (if applicable) shall be governed by Option 2 (General Authorization) and provide for a 14-day advance notice; and (iii) for Clauses 17 and 18, the Parties choose Ireland and the Supervisory Authority of Ireland.

For purposes of the UK SCC Addendum, the Parties (i) select the Approved EU SCCs, including the Appendix, in Table II and (ii) select both Importer and Exporter in Table 4. Annexes I and II of the 2021 EU SCCs are attached hereto as Exhibit 1 and shall serve to provide the information required for Table 1 of the UK SCC Addendum.

For the purposes of the Swiss SCC Addendum, (i) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the 2021 EU SCCs; (ii) the references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP; (iii) the Federal Data Protection and Information Commissioner of Switzerland shall be the competent supervisory authority in Annex I.C under Clause 13 of the 2021 EU SCCs, where the transfer of Personal Data is subject to the FADP.

In the event of any direct conflict between this Addendum and the 2021 EU Standard Contractual Clauses, the UK SCC Addendum or the Swiss SCC Addendum, the 2021 EU Standard Contractual Clauses, UK SCC Addendum and Swiss SCC Addendum (as applicable) shall prevail.

8. Requests from Data Subjects

Processor will make available to Controller the Personal Data of its Data Subjects and the ability to fulfill requests by Data Subjects to exercise one or more of their rights under Applicable Data Protection Laws in a manner consistent with Processor's role as a Data Processor. Processor will provide reasonable assistance to assist with Controller's response.

If Processor receives a request directly from Controller's Data Subject to exercise one or more of their rights under Applicable Data Protection Laws, Processor will direct the Data Subject to Controller unless prohibited by law.

9. Security

Each party shall implement and maintain appropriate technical and organizational practices designed to protect Personal Data against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such security practices shall be consistent with those set forth in the CS Group Services Security Exhibit, which is available at https://www.citrix.com/buy/licensing/citrix-services-security-exhibit.html.

10. Personal Data Breach

A party acting as a Processor shall notify Controller without undue delay after becoming aware of a Personal Data Breach involving Personal Data in Processor's possession, custody or control. Such notification shall at least: (i) 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; (ii) provide the name and contact details of the data protection officer or other contact where more information can be obtained; and (iii) 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. The parties will coordinate on the content of any public statements or required notices to individuals and/or supervisory authorities.

11. Instructions and Providing Information & Assistance

Controller may provide additional instructions to Processor related to the Processing of Personal Data that are necessary for the parties to comply with their respective obligations under Applicable Data Protection Laws as a Data Controller and Data Processor. Processor will comply with Controller's instructions at no additional charge, provided that in the event that the instructions impose costs on Processor beyond those included in the scope of Services under the Agreement, the parties agree to negotiate in good faith to determine the additional costs. Processor will promptly inform Controller if it believes that Controller's instructions are not consistent with Applicable Data Protection Laws, provided that Processor shall not be obligated to independently inspect or verify Controller's Processing of Personal Data.

Processor will provide Controller with information reasonably necessary to assist Controller in enabling Controller's compliance with its obligations under Applicable Data Protection Laws, including without limitation Processor's obligations under the GDPR to implement appropriate data security measures, carry out a data protection impact assessment and consult the competent supervisory authority (taking into account the nature of Processing and the information available to Processor), and as further specified in this DPA.

12. Return and Deletion of Personal Data

A party acting as a Processor will return or provide an opportunity for Controller to retrieve all Personal Data after the end of the Agreement and delete existing copies. Controller shall have thirty (30) calendar days to download its Personal Data after termination of the Agreement and must contact Processor for download access and instructions. In the event Controller does not contact Processor for this purpose within 30 calendar days, Processor shall delete Controller's Personal Data promptly once that Personal Data is no longer accessible by Controller, except for (i) 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 this DPA until such data has been deleted.

13. Audit

In the event the information Controller requests of Processor under Section 11 above does not satisfy Controller's obligations under Applicable Data Protection Laws, Controller may carry out an audit of Processor's Processing of Your Personal Data up to one time per year or as otherwise required by Applicable Data Protection Laws. To request an audit, Controller must provide Processor with a proposed detailed audit plan three weeks in advance, and the parties will work with You in good faith to agree on a final written plan. Any such audit shall be conducted at

Controller's own expense, during normal business hours, without 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. If any of the requested scope of the audit is covered by an audit report issued to Processor by a qualified third-party auditor within the prior twelve months, then the parties agree that the scope of Controller's audit will be reduced accordingly.

Controller may use a third-party auditor with Processor's agreement, which will not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Processor. If the third party is Controller's supervisory authority that applicable law enables it to audit Processor directly, Processor will cooperate with and provide reasonable assistance to the supervisory authority in accordance with applicable law.

Controller will provide Processor with a copy of any final report unless prohibited by Applicable Data Protection Laws, will treat the findings as Confidential Information in accordance with the terms of the Agreement (or confidentiality agreement entered into between the parties), and use it solely for the purpose of assessing Processor's compliance with the terms of the Agreement, this DPA and Applicable Data Protection Laws.

14. Data Protection Officer

You may contact the CSG global Data Protection Officer c/o CSG Systems, Inc., 100 District Avenue, Burlington MA 01803 USA. If You have appointed a Data Protection Officer, You may include their contact information in the Agreement.

15. Term

This DPA becomes effective upon the later of Your execution of the Agreement and the version date of this DPA.

EXHIBIT A: 2021 EU SCC ANNEXES

ANNEX 1

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Cloud Software Group, Inc.

The contact information, signature and date provided above are incorporated herein by reference

Activities relevant to the data transferred under these Clauses: Services as described in the Agreement.

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Partner
The contact information, signature and date provided above are incorporated herein by reference

Activities relevant to the data transferred under these Clauses: Services as described in the Agreement.

Role (controller/processor): Controller / Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As needed in order for Partner to perform the Services, which may include:

- Employees and contractors
- Customers, prospects and end users
- Partners, agents, and representatives

Categories of personal data transferred

As needed in order for Partner to perform the Services, which may include:

- Direct identifiers such as first name, last name, date of birth, and home address
- Communications data such as home telephone number, cell telephone number, email address, postal mail, and fax number
- Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, and CV data
- Other data such as financial, goods or services purchased, device identifiers, online profiles, and IP address
- Details of user's interaction with the data importer's systems and with systems for which the data importer provides computing services
- Information that the data exporter or its users choose to include in files stored on or routed through data importer's applications
- Other Personal Data to which the Parties provide to each other in connection with the provision of Services

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Personal data transferred is determined and controlled by the data exporter and may include sensitive data such as government identifier, religious affiliation, or any other sensitive data necessary to be Processed in order to perform the Services.

Technical and organizational security measures are described in CSG Services Security Standards available at: https://www.citrix.com/buy/licensing/citrix-services-security-exhibit.html

The frequency of the transfer *(e.g., whether the data is transferred on a one-off or continuous basis).*

Transfers on a continuous basis as needed to perform the Services.

Nature of the processing

Please refer to Section 3 of the Addendum

Purpose(s) of the data transfer and further processing

Please refer to Section 3 of the Addendum

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Retained for the duration of the Services.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

Transfers on a continuous basis as needed to perform the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: Supervisory Authority of Ireland.
Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: Supervisory Authority of Ireland.
Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Supervisory Authority of Ireland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and organizational security measures are described in the CS Group Services Security Exhibit available at: https://www.citrix.com/buy/licensing/citrix-services-security-exhibit.html