Computacenter

DATA PROTECTION ADDENDUM

1. BACKGROUND

1.1 **Purpose and Effectiveness.** This Data Protection Addendum ("**DPA**") is incorporated into and forms part of a written (including in electronic form) Master Products and Services Agreement ("**Agreement**") between Provider and Customer. In consideration of the mutual obligations set out herein, Provider and Customer hereby agree that the terms and conditions set forth below shall be added as a DPA to, effective concurrently with, the Agreement. Except as expressly modified by this DPA, the terms of the Agreement and the terms of the Services to be provided under the Agreement shall continue in full force and effect.

1.2 **Application**. This DPA applies to Personal Data processed by Provider and its Subprocessors in connection with its provision of the Services under the Agreement. Provider agrees to process Personal Data in accordance with the relevant provisions of Applicable Data Protection Laws of which Provider has actual notice that Customer is subject in connection with the Services; provided, however, that such agreement shall not be interpreted or construed as an acknowledgment admission that Processor is itself subject to such Applicable Data Protection Laws.

2. DEFINITIONS

As used in this DPA, the following terms shall have the meanings set out below and capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Agreement.

2.1 **Applicable Data Protection Laws.** Applicable Data Protection Laws means the laws and regulations that are applicable to the Personal Data and the processing of Personal Data that are processed by Provider and its Subprocessors in providing the Services under the Agreement including, without limitation, to the extent applicable, the GDPR and the CCPA;

2.2 **CCPA**. The term "CCPA" means the California Consumer Privacy Act and, upon its effectiveness, the California Privacy Rights Act and regulations promulgated under either act.

2.3 **Controller.** Controller has the same meaning as set forth in the GDPR.

2.4 **Data Subject**. Data Subject means (i) an identified or identifiable natural person whose Personal Data is subject to the GDPR; (ii) a "Consumer" as the term is defined in the CCPA; or (iii) any other natural person whose personal information is protected under Applicable Data Protection Laws.

2.5 **GDPR**. The term "GDPR" means the General Data Protection Regulation 2016/679 and any national legislation which supplements the GDPR, together with binding guidance and codes of practice issued from time to time by relevant supervisory authorities applicable to the Member States of the European Economic Area ("EEA").

2.6 **Personal Data.** Personal Data means that subset of Confidential Information comprised of any personal data or personal information as defined in Applicable Data Protection Laws that is processed in connection with the Services provided by Provider under the Agreement. For clarity, the Personal Data includes, without limitation, the Personal Data of Customer, its employees and agents, or Customer's end users.

2.7 **Personal Data Breach.** Personal Data Breach means a confirmed (1) breach of security leading to the unauthorized destruction, loss, alteration, disclosure of, or access to, Personal Data of Customer or Customer's end users or (2) similar incident involving Personal Data of Customer or Customer's end users, in each case for which Customer is required under Applicable Data Protection Laws to provide notice to competent data protection authorities or Data Subjects.

2.8 **Processor/process/processing.** "Processor", "process", and "processing" have the same meanings as set forth in the GDPR, and their cognate and equivalent terms shall be construed accordingly.

2.9 **Subprocessor**. Subprocessor means any person (including any Provider Affiliate or third party but excluding any Provider Personnel)

appointed by Provider to process Personal Data in accordance with a statement of work and this Agreement.

2.10 **Restricted Transfer.** Restricted Transfer means a transfer of Personal Data from Customer or its Affiliate to Provider or its Affiliate, where such transfer would be prohibited by Applicable Data Protection Laws in the absence of an approved adequacy means for data protection such as the Standard Contractual Clauses;

2.11 **Standard Contractual Clauses.** Standard Contractual Clauses means the standard contractual clauses for the transfer of personal data to Processors established in third countries which do not ensure an adequate level of protection as set out in Commission Decision 2010/87/EU, as updated by the European Commission June 27, 2021, and as further updated, amended, replaced or superseded from time to time by the European Commission.

3. DESCRIPTION OF PERSONAL DATA PROCESSING

3.1 **Subject Matter and Duration.** The subject matter and duration of the processing of Personal Data corresponds with, and is dependent upon, the Services for which Customer engages Provider as defined in the Agreement and each applicable SOW.

3.2 **Nature and Purpose**. The SOW sets forth the scope of the Services. Any processing of Personal Data by Provider will take place in the course of delivering the Services.

3.3 **Types of Personal Data to be Processed.** The Services are Business-to-Business in nature and involve the following types of Personal Data including Special Categories of Data:

(a) Business contact information including Customer's personnel names, titles, gender, work address, work email, work telephone numbers, job title, and system access / usage / authorization data;

(b) If Customer selects Workforce Staffing Services, prospective personnel contact information of Provider's personnel may be provided (e.g. address, telephone number, email address), and typical resume information (e.g. employment history, skills, education, professional certifications and licensure, interests and preferences, and compensation matters);

(c) Personal Data that are either (i) exported by Customer (or Customer's service provider) to a segregated area in Provider's environment for purposes of the providing the Services or, (ii) residing within areas of Customer's environment that are configured by Customer to be accessible to Provider. In either case, such Personal Data may be accessible to Provider but are not directly used by Provider in the course of providing the Services; and

(d) Personal Data that is provided by Customer and/or accessed by Provider for the purpose of Provider's performing help desk services to Customer (e.g. name, phone number, IP address).

(e) Personal Data provided pursuant to a statement of work for configuration or implementation of a system requiring collection and input of Personal Data such as implementation of Voice over IP (VoIP) systems for Customer (requiring e.g. contact name, office phone number, office address and job title).

(f) The Personal Data made accessible by Customer to Provider may include Special Categories of Data (as defined in the GDPR) including, by way of example and not in limitation, financial and financial account data, data concerning health if Customer is a health care provider or in the medical/pharmaceutical industry, or academic matters if Customer is an educational institution.

3.4 **Categories of Data Subjects.** Customer may submit Personal Data for the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, without limitation, Personal Data relating to the following categories of Data Subjects: (i) personnel and prospective personnel of Customer and its customers, contractors, vendors, and business partners, and (ii) other natural persons whose Personal Data may be accessible to Provider in the course of providing the Services as described in Section 3.3(c), (d), or (e) of this DPA.

3.5 **Processing Operations/Purpose**. The specific processing operations and purposes thereof that comprise the Services are set forth in each SOW. In general, Personal Data may be subject to the following basic processing activities: communications with Data Subjects, for example, to provide consulting and support Services; access to Customer's network (including Personal Data therein) to design,

implement, operate, network monitoring and troubleshooting; storage and backup of Customer data; and data transmission, retrieval, and access.

4. PROVIDER OBLIGATIONS

4.1 **Instructions from Customer**. The parties agree that Provider processes Customer Personal Data for Customer as a Processor or service provider as such terms are defined under the GDPR and CCPA, respectively. Provider will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each SOW and each use of the Services then constitutes further instructions. Provider will use reasonable efforts to follow any other Customer instructions, as long as they are required by Applicable Data Protection Laws, technically feasible, and do not require changes to the Services. If any of the before-mentioned exceptions apply, or Provider otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Applicable Data Protection Laws, Provider will immediately notify Customer (email permitted).

4.2 **Legal Requirement to Process**. Provider may also process Personal Data where required to do so by applicable law to which Provider or any Provider Affiliate is subject, in which case Provider shall inform Customer of that legal requirement before such processing, unless that law prohibits such information on important grounds of public interest (e-mail permitted).

4.3 **Provider Personnel.** Provider shall only grant access to Personal Data to Provider Personnel who commit themselves to contractual or statutory obligations of confidentiality, and shall train Personnel having access to Personal Data in applicable data security measures.

4.4 **Security**. Provider shall maintain commercially reasonable technical and organizational measures for protection of the security of the Personal Data and the processing thereof (including protection against unauthorized or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data),

4.5 **Subprocessors**. Provider shall have a written agreement in place with each Subprocessor providing that the Subprocessor is subject to obligations and requirements with respect to Personal Data comparable in scope to those imposed on Provider in the Agreement and in this DPA. Provider shall remain responsible to Customer for any failure of its Subprocessor to fulfil its obligations in relation to the processing of Personal Data.

4.6 **Cooperation**. At Customer's request, Provider will reasonably cooperate with Customer in dealing with requests from Data Subjects or regulatory authorities regarding Provider's processing of Personal Data. Provider shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. Provider shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Applicable Data Protection Laws. Where such functionality is not provided, Provider will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Applicable Data Protection Laws.

4.7 **Personal Data Breach Notification**. Provider will notify Customer without undue delay after becoming aware of any Personal Data Breach, provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Applicable Data Protection Laws, and will reasonably cooperate with Customer or regulatory authorities regarding any Personal Data Breach. Provider may provide such information in phases as it becomes available. Such notification or cooperation shall not be interpreted or construed as an admission of fault or liability by Provider. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breach.

4.8 **Documentation and Records of Processing**. Provider shall make available to Customer on request all documentation reasonably necessary to demonstrate compliance with this DPA and, where required by Applicable Data Protection Laws, all records maintained by Provider relating to the processing of Personal Data, subject to Provider withholding access to any records containing confidential information pertaining to other customers of Provider. Provider shall not be required to make such documentation available to Customer more than once in any twelve month period except under the circumstances identified in Section 6.2(a).

4.9 **Data Protection Impact Assessment**. If, pursuant to Applicable Data Protection Laws, Customer is required to perform a data protection impact assessment or prior

consultation with a regulator, at Customer's request, Provider will provide such documents as are generally available for the Services (for example, this DPA, the Agreement, existing audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4.10 **Personal Data Deletion**. Upon termination of the Agreement, (a) Customer shall have exported or deleted all Personal Data in Provider's systems that are accessible to Customer or arranged with Provider to do so, and (b) Provider shall cease processing the Personal Data except to the extent required by this clause. Customer hereby instructs Provider to delete any Personal Data remaining on Provider's servers within a reasonable time period following termination of the Agreement. Provider shall protect any Personal Data not so deleted in accordance with this DPA.

5. CUSTOMER OBLIGATIONS

5.1 **Customer Affiliates.** Customer shall serve as a single point of contact for Provider and be solely responsible for internal coordination, review, and submission of any processing instructions in respect of which any Customer Affiliate is the Controller.

5.2 **Customer's Compliance Responsibilities**. Customer represents and warrants that:

(a) Except as set forth in the Agreement and this Addendum, and to the extent within the control of Customer, Customer is solely responsible for its Personal Data, including without limitation, the security of such Personal Data;

(b) Customer has the necessary authority rights and licenses, consents, permissions, waivers and releases to use the Personal Data, to transfer or otherwise make the Personal Data accessible to Provider, and to enable Provider to process the Personal Data as intended by the parties to provide the Services in accordance with the Agreement;

(c) Customer has a legally sufficient privacy policy or privacy notice that is made available to customers prior to their provision of any Personal Data to Customer or Provider;

(d) To Customer's knowledge, processing by Provider of Customer Personal Data:

(i) does not violate, misappropriate or infringe any rights of Provider or any third party,

(ii) does not constitute defamation, invasion of privacy or publicity, or otherwise violate any rights of any third party, and

(iii) is not designed for use in any illegal activity or does not promote illegal activities, including, without limitation, in a manner that might be illegal or harmful to any person or entity; or

(iv) does not distribute, share, or facilitate the distribution of unauthorized data, malware, viruses, Trojan horses, spyware, worms, or other malicious or harmful code.

5.3 **Customer's Security Responsibilities**. Customer agrees that, without prejudice to Provider's obligations under Section 5.1 (Provider's Security Measures, Controls and Assistance) and Section 5.2 (Personal Data Breach):

(a) Customer is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services;

(iii) securing Customer's systems and devices as used in connection with the Services; and

(iv) backing up its Personal Data.

(b) Provider has no obligation to protect Personal Data that Customer elects to store or transfer outside of Provider's and its Subprocessors' systems (for example, offline or on-premises storage).

5.4 **Customer's Security Assessment.**

(a) Customer is solely responsible for evaluating for itself whether the Services and Provider's obligations under this Addendum will meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws.

(b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Personal Data as well as the risks to individuals), Provider's obligations under this Addendum provide a level of security appropriate to the risk in respect of the Personal Data.

5.5 Authority. Customer shall ensure that, wherever it discloses Personal Data to Provider for the purposes of Provider processing that Personal Data to provide the Services, it is authorized to do so in accordance with the Applicable Data Protection Laws.

6. ADDITIONAL PROVISIONS APPLICABLE TO PROCESSING OF PERSONAL DATA SUBJECT TO THE GDPR

This Section 6 applies only to processing of Personal Data that is subject either to (a) the GDPR or (b) Applicable Data Protection Laws in effect in Switzerland, the United Kingdom, or other countries that regulate Subprocessors, Processor audits, or Restricted Transfers in a manner substantially similar to the GDPR.

6.1 Subprocessors

(a) Provider is expressly and specifically authorized to use (i) those Subprocessors already engaged by Provider or any Provider Affiliate as at the date of this Agreement; (ii) any Provider Affiliate as a Subprocessor.

Provider is generally authorized to engage any other Subprocessor for the provision of goods and/or services to the Customer pursuant to the Agreement(s) and for the Operation and maintenance of Provider systems processing Customer data

(b)

6.2 Certifications and Audits

(a) **Customer Audit.** Customer or its qualified and independent third party auditor reasonably acceptable to Provider (which shall not include any third party auditors who are either a competitor of Provider) may audit Provider's control environment and security practices relevant to Personal Data processed by Provider only if:

i. Provider has not provided sufficient documentation pursuant to Section 4.6 of its compliance with the technical and organizational measures that protect the production systems of the Services through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) other valid recognized attestation report;

ii. A Personal Data Breach has occurred;

iii. An audit is formally requested by Customer's data protection authority; or

iv. Applicable Data Protection Laws provide Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless Applicable Data Protection Laws requires more frequent audits.

(b) **Scope of Audit.** Customer shall provide at least sixty (60) days advance notice of any audit unless mandatory Applicable Data Protection Laws or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Notwithstanding the foregoing, if the physical data center(s) where the Personal Data is processed is not accessible to Customer, Provider will make available, via secure conference, various documents which attest to the security posture of such facility. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Provider.

(c) **Cost of Audits.** Customer shall bear the costs of any audit unless such audit reveals a material breach by Provider of this DPA, then Provider shall bear its own expenses of an audit. If an audit determines that Provider has breached its obligations under the DPA, Provider will promptly remedy the breach at its own cost.

6.3 Restricted Transfers

(a) In respect of any Restricted Transfer,

the parties hereby enter into the Standard Contractual Clauses, Module 2 (Controller to Processor). The Data Exporter shall be Customer and any Customer Affiliate that Customer allows to use the Services. The Data Importer shall be the Provider and any Provider Affiliate that supports the Services. Annex 1 to the Standard Contractual Clauses shall be deemed to be prepopulated with Section 3 of this DPA. Annex 2 to the Standard Contractual Clauses shall be deemed to be prepopulated with the following "*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 for the rights and freedoms of natural persons, Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate the specific controls described in Article 32(1), (a) to (d) inclusive of the GDPR.*

(b) The Standard Contractual Clauses shall come into effect on the commencement of a Restricted Transfer among any parties to the Standard Contractual Clauses and shall be governed by the law of the country in which Customer (or its relevant Customer Affiliate) is established by law.

7. PRECEDENCE

The provisions of this DPA are supplemental to the provisions of the Agreement. In the event of inconsistencies between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail. To the extent that there is any conflict or inconsistency between the terms of the Standard Contractual Clauses and the terms of this DPA or the Agreement, the terms of the Standard Contractual Clauses shall take precedence.

8. SEVERANCE

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible; or (ii) if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.