DATA PROCESSING ADDENDUM

Last updated: October 7, 2022

This Data Processing Addendum ("**DPA**") forms part of the Agreement between the party identified in the Agreement ("**Customer**") and VMware and applies if VMware processes Personal Data on behalf of Customer while providing Services. This DPA does not apply where VMware is the Controller. All capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement.

1. PROCESSING

1.1. Role of the Parties. VMware will process Personal Data under the Agreement only as a Processor acting on behalf of Customer. Customer may act either as a Controller or as a Processor of Personal Data. If Customer is acting as a Processor, Customer must communicate with VMware about the Processing on behalf of the Controller, and VMware will direct any inquiries from the Controller to Customer.

1.2. Customer Processing of Personal Data. Customer's use of the Services and processing instructions must comply with Data Protection Law and Customer must obtain all rights and authorizations necessary for VMware to process Personal Data under the Agreement.

1.3. VMware Processing of Personal Data.

1.3.1. VMware must comply with Data Protection Laws applicable to its provision of the Services and will process Personal Data in accordance with Customer's documented instructions. Customer agrees that the Agreement is its complete and final instructions to VMware regarding the processing of Personal Data. Processing any Personal Data outside the scope of the Agreement requires prior written agreement between VMware and Customer and may incur additional fees. Customer may terminate the Agreement upon written notice if VMware declines or is unable to accept any reasonable modification to processing instructions that (a) are necessary to enable Customer to comply with Data Protection Laws, and (b) the parties were unable to agree upon after good faith discussions.

1.3.2. If the California Consumer Privacy Act of 2018, as amended, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**") applies to any Personal Data that Customer discloses to VMware for a 'business purpose' and where VMware is acting as Customer's 'service provider', as such terms are defined under CCPA, then VMware will not retain, use, or disclose Personal Data for commercial or any other purposes other than for the specific purpose of providing the Services or as otherwise permitted by the CCPA.

1.4. Processing of Personal Data Details.

1.4.1. **Subject matter**. The subject matter of the processing under the Agreement is Personal Data.

1.4.2. **Duration.** The duration of the processing under the Agreement is determined by Customer and as set forth in the Agreement.

1.4.3. **Purpose.** The purpose of the processing under the Agreement is the provision of the Services by VMware to Customer as specified in the Agreement.

1.4.4. **Nature of the processing.** VMware and its Sub-processors are providing Services and fulfilling contractual obligations to Customer as described in the Agreement. These Services may include the processing of Personal Data by VMware and its Sub-processors.

1.4.5. **Categories of data subjects.** Customer determines the data subjects, which may include Customer's end users and customers, employees, contractors, suppliers, and other third parties.

1.4.6. **Categories of data.** Customer controls the categories of Personal Data that it submits to the Services through its use and configuration of the Services.

2. SUBPROCESSING.

2.1. Use of Sub-Processors. Customer authorizes VMware to engage Sub-processors to process Personal Data to provide the Services. VMware is responsible for any acts, errors, or omissions of its Sub-processors to the same extent VMware would be liable if performing the Services directly under the terms of the Agreement.

2.2. Obligations. VMware will enter into an agreement requiring each Sub-processor to process Personal Data in a manner substantially similar to the standards in the DPA, and at a minimum, at the level required by Data Protection Law.

2.3. **Notice.** VMware's list of Sub-processors is available at www.vmware.com/agreements/sub-processors.html or upon written request.

2.4. **Changes to Sub-processors.** VMware will provide prior notice to Customer of any new Sub-processor if Customer has subscribed to receive notification at www.vmware.com/agreements/sub-processors.html. If Customer objects to a new Sub-processor on reasonable data protection grounds within 10 days of receiving notice, VMware will discuss those concerns with Customer in good faith with a view to achieving resolution.

3. SECURITY MEASURES.

3.1. **Security Measures by VMware.** VMware will implement and maintain appropriate technical and organizational security measures designed to protect against Personal Data Breaches and to preserve the confidentiality, integrity, and availability of Personal Data ("**Security Measures**"). Security Measures are subject to technical progress and development. VMware may modify Security Measures from time to time, provided that any modifications do not result in material degradation of the overall security of the Services.

3.2. **Security Measures by Customer.** Customer must implement appropriate technical and organizational measures in its use and configuration of the Services.

3.3. **Personnel.** VMware restricts its personnel from processing Personal Data without authorization (except as required by applicable law). Any person authorized by VMware to process Personal Data is subject to confidentiality obligations.

4. PERSONAL DATA BREACH RESPONSE.

Upon becoming aware of a Personal Data Breach, VMware will notify Customer without undue delay and will provide information relating to the Personal Data Breach as reasonably requested by Customer. VMware will use reasonable endeavors to assist Customer to mitigate, where possible, the adverse effects of any Personal Data Breach.

5. AUDIT REPORTS.

VMware (or third parties engaged by VMware) audits its compliance against data protection and information security standards on a regular basis. VMware's security certifications are published at www.vmware.com/products/trust-center.html. Upon Customer's written request, VMware will provide Customer with a summary of the current audit report or other documentation generally made available by VMware for Customer to verify VMware's compliance with this DPA.

6. PERSONAL DATA TRANSFERS.

6.1. **Personal Data Transfers.** VMware may transfer and process Personal Data to and in locations around the world where VMware or its Sub-processors maintain data processing operations to provide the Services.

6.2. **Personal Data Transfers from the European Economic Area, the United Kingdom, and Switzerland.** VMware has achieved Binding Corporate Rules ("**BCR**") for Personal Data it processes as a Processor. VMware's BCR is available at www.vmware.com/help/privacy/binding-corporate-rules.html. VMware will process all European Economic Area, United Kingdom, and Switzerland Personal Data transferred to it for processing under the Agreement in accordance with its BCR, including where Personal Data is processed outside of the European Economic Area by VMware, any member of its group of companies, or any external Sub-processor.

6.3. **BCR Enforcement.** Customer has the right to enforce the BCR against VMware International Unlimited Company or any member of VMware's group of companies for breaches of the BCR they caused, subject to the terms of the Agreement (including its exclusions and limitations) for the benefit of the members of VMware's group of companies. Customer is the sole entity responsible for coordinating all communications with and claims against any member of the VMware group of companies. Customer must make and receive any communication on behalf of its affiliates.

7. DELETION OF PERSONAL DATA.

Following expiration or termination of the Agreement, VMware will delete or return to Customer all Personal Data as set forth in the Agreement. If VMware is required by applicable law to retain Personal Data, VMware will implement reasonable measures to prevent any further processing. The terms of this DPA will continue to apply to that retained Personal Data.

8. COOPERATION.

8.1. **Data Subject Requests.** If VMware receives any requests from individuals wishing to exercise their rights in relation to Personal Data processed under the Agreement (a "**Request**"), VMware will promptly redirect the Request to Customer. VMware will not respond to the Request directly unless

authorized by Customer or required by law. VMware will reasonably cooperate with Customer, at Customer's expense, if Customer cannot address the Request using the Services.

8.2. **DPIAs and Prior Consultations.** If required by Data Protection Law, VMware will, with reasonable notice and at Customer's expense, provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments ("**DPIAs**") and prior consultations with data protection authorities.

8.3. **Legal Disclosure Requests.** If VMware receives a valid request for the disclosure of Personal Data that is subject to this DPA, that request will be addressed in accordance with the Agreement.

9. GENERAL.

9.1. **Relationship with Agreement.** Any claims brought under this DPA will be subject to the terms of the Agreement (including its exclusions and limitations).

9.2. **Conflicts.** In the event of any conflict between this DPA and any provisions in the Agreement, the terms of this DPA will prevail.

9.3. **DPA Updates.** VMware may update this DPA: (a) if required to do so by a data protection authority or other government or regulatory entity; or (b) to comply with Data Protection Law. VMware may further exchange, adopt, or update its data transfer or compliance mechanisms provided they are recognized by Data Protection Law. The modified DPA will become effective when published on VMware's website or as otherwise provided in the Agreement.

10. DEFINITIONS

Agreement means the written or electronic agreement between Customer and VMware for the provision of Services to Customer.

Controller means an entity that determines the purposes and means of the processing of Personal Data.

Data Protection Law means all data protection and privacy laws applicable to the processing of Personal Data in relation to the Services.

Demand means a subpoena, court order, agency action, or any other legal or regulatory requirement to disclose any Customer Content.

GDPR means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

Personal Data means any information relating to an identified or identifiable natural person contained within Customer Content.

Personal Data Breach means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Processor means an entity that processes Personal Data on behalf of a Controller.

Services means, for the purposes of this DPA, any Cloud Service or Support Services provided by VMware to Customer pursuant to the Agreement.

Sub-processor means any Processor engaged by VMware or any member of its group of companies that processes Personal Data pursuant to the Agreement. Sub-processors may include third parties or any member of VMware's group of companies.

[Continued on next page]

vmware®

GDPR Supplemental Measures Addendum to Data Processing Addendum

This GDPR Supplemental Measures Addendum ("**Supplemental Measures Addendum**") supplements the DPA and reflects the supplemental measures of VMware if VMware processes Personal Data within the scope of GDPR on Customer's behalf. Nothing in this Supplemental Measures Addendum is intended to restrict the commitments contained in the DPA. All capitalized terms used but not defined in this Supplemental Measures Addendum will have the meanings set forth in the DPA.

1. Warranty.

1.1. The parties warrant that they have no reason to believe the laws and practices in the third country of destination applicable to the processing of Personal Data by VMware, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent VMware from fulfilling its obligations under section 2 (Notification in case of Required Disclosures and direct access). This warranty is based on the understanding that this section 1 (Warranty) is not in contradiction to the laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR.

1.2. VMware agrees to notify Customer promptly if VMware has reason to believe that VMware is or has become subject to laws or practices not in line with the requirements under section 1.1, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in section 1.1.

1.3. Following a notification pursuant to section 1.2, or if Customer otherwise has reason to believe that VMware can no longer fulfil its obligations under section 1, Customer shall promptly identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by Customer or as requested by Customer to be implemented by VMware in accordance with section 1.3.1 of the DPA. Customer shall suspend the data transfer if Customer considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent data protection authority to do so, and Customer shall be entitled to terminate the Agreement, insofar as it concerns the processing of Personal Data under this section 1 (Warranty).

2. Notification in case of Required Disclosures and direct access.

2.1. If VMware is required by a Demand or where VMware becomes aware of any direct access by public authorities to Personal Data transferred pursuant to our Agreement, unless legally prohibited from doing so, VMware will:

(a) provide Customer with notice and a copy of the Demand as soon as practicable;

(b) inform the relevant government authority that VMware is a service provider acting on Customer's behalf and all requests for access to Customer Content should be directed in writing to the contact person Customer identifies to VMware (or if no contact is timely provided, VMware will direct the relevant governmental authority generally to Customer's legal department); and

(c) only provide access to Customer Content with Customer's authorization.

2.2. Where permissible under the laws of the country of destination, VMware agrees to provide Customer, at regular intervals for the duration of the Agreement, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority, whether requests have been challenged and the outcome of such challenges).

2.3. VMware will preserve the information pursuant to section 1 (Warranty) for the duration of the Agreement and make it available to the competent data protection authority on request.

2.4. Sections 2.1 and 2.2 are without prejudice to VMware's obligation under sections 1.1 and 1.2 to inform Customer promptly where VMware is unable to comply with the obligations in these sections.

3. Review of legality and data minimization in case of public authority access requests.

3.1. If VMware is required by a Demand, VMware will review the legality of the request for disclosure (whether it remains within the powers granted to the requesting public authority), and challenge the request if VMware considers that there are reasonable grounds to consider that the request is unlawful.

3.2. When challenging a request, VMware shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on the merits of the case. VMware shall not disclose Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to VMware's obligations to notify

Customer if VMware has reason to believe that it is or has become subject to laws or practices not in line with the requirements of section 1.1.

3.3. VMware will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to Customer. VMware shall make its assessment available to the competent data protection authority on request.

3.4. VMware agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.