NVIDIA CLOUD SERVICES

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") supplements the Agreement governing NVIDIA's Processing of Personal Data in User Content uploaded by Customer ("Customer Data") in connection with Customer's use of the NVIDIA services that is the subject of the Agreement (the "Services"). All capitalized terms not defined in this DPA will have the meaning given to them in the Agreement.

DEFINITIONS

"Data Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

"Data Processor" means the natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws" means all applicable laws and regulations regarding the Processing of Personal Data.

"Data Subject" means an identified or identifiable natural person.

"Data Subject Request" means requests or objections made by Data Subjects pursuant to Data Protection Laws.

"Personal Data" means any information relating to a Data Subject, uploaded by or for Customer or Customer's agents, employees, or contractors to the Services as Customer Data.

"Process," "Processed," or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Security Incident" means a breach of NVIDIA's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

"Sub-Processor" means any legal person or entity engaged in the Processing of Personal Data by Data Processor.

1. SCOPE OF THE PROCESSING

1.1 ROLES. NVIDIA will act as Data Processor to Customer. Customer will act as Data Controller (unless Customer is a Data Processor, in which case NVIDIA will act as a Sub-Processor to Customer). Each party will comply with Data Protection Laws in the performance of this DPA. Customer acts as a single point of contact and shall obtain any relevant authorizations, consents and permissions for the processing of Personal Data by NVIDIA in accordance with this DPA.

1.2 INSTRUCTIONS. The Agreement constitutes Customer's initial written instructions to NVIDIA for Processing of Personal Data. Customer may issue additional or alternate instructions provided that such instructions are agreed in writing between Customer and NVIDIA.

1.3 NATURE, SCOPE AND PURPOSE OF THE PROCESSING. NVIDIA will only Process Personal Data in accordance with Customer's instructions, as explicitly authorized in writing, or as required under applicable law provided that NVIDIA will inform Customer of the legal requirements before Processing. Customer acknowledges all Personal Data it instructs NVIDIA to Process for the purpose of providing Services must be limited to the

Customer Data Processed within the Services. Details of the Processing of Customer Data conducted under this DPA are set forth in Appendix 1.

2. DATA PROCESSOR

2.1 DATA CONTROLLER'S INSTRUCTIONS. Given the nature of the processing, Customer agrees that it is unlikely that NVIDIA would be aware that compliance with Customer's instructions would result in a violation of Data Protection Laws. However, where NVIDIA believes compliance with Customer's instructions would result in a violation of Data Protection Laws, NVIDIA will promptly notify Customer thereof.

2.2 DATA PROCESSOR PERSONNEL. Persons authorized by NVIDIA to Process Personal Data will be bound by appropriate confidentiality obligations.

2.3 DATA SECURITY MEASURES. NVIDIA will maintain appropriate technical and organizational safeguards to protect the security, confidentiality, and integrity of Customer Data, including any Personal Data contained therein, as set forth in Section 5.

2.4 DATA PROCESSOR ASSISTANCE. NVIDIA will assist Customer as reasonably requested by Customer to facilitate Customer's compliance with obligations under Data Protection Laws in connection with NVIDIA's Processing of Personal Data, taking into account the nature of Processing and information available to NVIDIA.

3. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

3.1 DATA SUBJECT RIGHTS. Each party will abide by Data Protection Laws and will ensure transparent information and appropriate channels for the exercise of the rights of a Data Subject, including during the collection of Personal Data or when responding to Data Subject Requests.

3.2 REQUESTS FROM DATA SUBJECTS. Unless prohibited by law, NVIDIA will promptly notify Customer of any Data Subject Requests and Customer hereby authorizes NVIDIA to inform the Data Subject that the Customer has been notified.

3.3 RESPONSES. Customer will be solely responsible for responding to Data Subjects in respect of any Data Subject Requests. NVIDIA will reasonably support Customer in relation to Data Subject Requests such as by forwarding any Data Subject Requests to Customer. i

3.4. REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry, or investigation by a government body, data protection authority, or law enforcement agency regarding the Processing of Personal Data, NVIDIA will promptly notify Customer unless prohibited by applicable law. If any government body, data protection authority, or law enforcement agency sends NVIDIA a demand for Customer Data, NVIDIA will attempt to redirect such authority to request that data directly from Customer. As part of this effort, Customer hereby authorizes NVIDIA to provide Customer's basic contact information to such authority. If NVIDIA is legally required to disclose Customer Data to a government body, data protection authority, or law enforcement agency, then NVIDIA will notify Customer without undue delay of the demand to allow Customer to seek a protective order or other appropriate remedy unless NVIDIA is legally prohibited from doing so.

3.5 ASSISTANCE. At Customer's request, NVIDIA will provide reasonable assistance and cooperation to Customer in the preparation of any response to Data Subject Request or to requests from authorities taking into account the nature of the Processing by NVIDIA.

4. SECURITY INCIDENT

4.1 NOTIFICATION. NVIDIA will notify Customer of a Security Incident commensurate with applicable laws and regulations, without undue delay after becoming aware of the Security Incident that relates to the Customer Data. NVIDIA will take appropriate measures to investigate and address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident. NVIDIA's notification of, or response to, a Security Incident is not an acknowledgment by NVIDIA of any fault or liability with respect to the Security Incident.

4.2 NVIDIA ASSISTANCE. To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), NVIDIA will cooperate with and assist Customer by including in the notification under Section 4.1 such information about the Security Incident as NVIDIA is able to disclose to Customer, taking into account the nature of the processing, the information available to NVIDIA, and any restrictions on disclosing the information, such as confidentiality.

4.3 UNSUCCESSFUL SECURITY INCIDENTS. Customer agrees that an unsuccessful Security Incident will not be subject to this Section 4. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of NVIDIA's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

4.4 COMMUNICATION. Notification(s) of Security Incidents to impacted Customer, if any, will be delivered to one or more of Customer's administrators by any means NVIDIA selects, including via encrypted email or other secured method. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on NVIDIA partner portal (https://partners.nvidia.com) at all times.

5. TECHNICAL AND ORGANIZATIONAL MEASURES

NVIDIA will implement and maintain appropriate technical and organizational measures (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) as set forth in the Security Standards in Appendix 2. Given the nature of the Processing, Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Services as described in the Security Standards meet Customer's requirements, including any of its security obligations under applicable Data Protection Laws. By entering into this DPA, Customer acknowledges and agrees that the technical and organizational measures implemented and maintained by NVIDIA provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled or within a NVIDIA virtual machine or application). NVIDIA may change the technical and organizational measures as described in the Security Standards at any time without notice so long as any new or additional measures serve the same purpose without diminishing the security level protecting Personal Data.

6. SUB-PROCESSORS

6.1 USE OF SUB-PROCESSORS. Customer authorizes NVIDIA to engage Sub-Processors appointed in accordance with this Section 6. NVIDIA engages, as applicable, the Sub-Processers listed in Appendix 3 below in respect of the Services. 6.2 NEW SUB-PROCESSORS. Prior to NVIDIA engaging a new Sub-Processor for the Services, NVIDIA

will (a) notify Customer by email to Customer's designated contact in the NVIDIA Support Portal, or by notification within the NVIDIA Support Portal (or other mechanism used to notify its customer base); and (b) provide the notice described in the preceding sentence at least 30 days before engaging a Sub-Processor with respect to existing Services which Customer has purchased. If a new Sub-Processor is engaged to support new Services or a new feature of the existing Services, then the notice described in this Section will be provided at or before the time such feature or Services are made generally available.

6.3 RIGHT TO OBJECT. To object to a Sub-Processor, Customer can: (a) terminate the Agreement by providing a written notice to NVIDIA, such termination shall take effect no later than 30 days from the date of NVIDIA's notice to Customer informing Customer of the new Sub-Processor. If Customer does not terminate the Agreement within this 30 days period, Customer is deemed to have accepted the new Sub-Processor; or (b) cease using the Services for which NVIDIA has engaged the Sub-Processor.

6.4 SUB-PROCESSOR OBLIGATIONS. Where NVIDIA authorizes a Sub-Processor as described in Section 6.1: (a) NVIDIA will restrict the Sub-Processor's access to Customer Data only to what is necessary to provide or maintain the Services, and NVIDIA will prohibit the Sub-Processor from accessing Customer Data for any other purpose; (b) NVIDIA will enter into a written agreement with the Sub-Processor and, to the extent that the Sub-Processor performs the same data Processing Services provided by NVIDIA under this DPA, NVIDIA will impose on the Sub-Processor the same contractual obligations that NVIDIA has under this DPA; and (c) NVIDIA will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-Processor that cause NVIDIA to breach any of NVIDIA's obligations under this DPA.

7. INTERNATIONAL DATA TRANSFERS

7.1 TRANSFER MECHANISM. If and to the extent there is a transfers any Customer Data as necessary to operate Services including trouble shooting, the transfer of Personal Data from the European Economic Area ("EEA"), the United Kingdom or Switzerland to a country located outside of the EEA which is not subject to an adequacy decision (a "Data Transfer") will be subject to the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as annexed to Commission Implementing Decision 2021/914 ("SCCs"), which are incorporated into this DPA by this reference (and, in relation to the United Kingdom or Switzerland, as amended or supplemented in accordance with this Section 7).

7.2 APPLICATION OF SCCs.

7.2.1 Modules. Module Two (Data Controller to Data Processor) will apply to a Data Transfer when Customer is a Data Controller. Module Three (Data Processor to Data Processor) will apply to a Data Transfer when Customer is a Data Processor.

7.2.2 Optional provisions. Where the SCCs identify optional provisions:

(a) in Clause 7 (Docking Clause) – the optional provision does not apply;

(b) in Clause 9(a) (Use of Sub-Processors) – Option 2 applies (and the parties will follow the process and timings agreed in the DPA to appoint Sub-Processors);

(c) in Clause 11(a) (Redress) – the optional provision does not apply;

(d) in Clause 17 (Governing law) – option 1 applies, and where the Agreement is governed by the laws of an EU Member State, the laws of that EU Member State apply; otherwise, law of Finland applies; and

(e) in Clause 18(b) (Choice of forum and jurisdiction) – where the Agreement is subject to the jurisdiction of the courts of an EU Member State, the courts of that EU Member State have jurisdiction; otherwise, the courts of Finland, Helsinki have jurisdiction.

7.2.3 Annexes of SCCs.

(a) In Annex 1A: the data exporter(s) is the Customer and its Affiliates making the Data Transfer (the "Data Exporter") and the data importers are NVIDIA entities receiving the Data Transfer (the "Data Importer"). The full name, address, and contact details for the Data Exporter and the Data Importer are set out in the Agreement, or can be requested by either party.

(b) In Annex 1B: The: relevant details are those set out in the Agreement, including Appendix 1 “Details of Processing” of this DPA.

(c) In Annex 1C: The competent supervisory authority is the supervisory authority applicable to the Customer (or, where relevant, applicable to the Customer’s representative).

(d) In Annex 2: the security provisions contained in Appendix 2 or other security related provisions in the Agreement apply.

7.3 INTERACTION WITH THE AGREEMENT. All notices, requests, monitoring/audit rights, conduct of claims, liability, and erasure or return of data relating to the SCCs will be provided/managed/interpreted, as applicable, in accordance with the relevant provisions in the Agreement, to the extent that such provisions do not conflict with the SCCs.

7.4 TRANSFERS SUBJECT TO SWISS DATA PROTECTION LAW. If there is a Data Transfer subject to Data Protection Laws of Switzerland, then the SCCs will apply with the following modifications: the competent supervisory authority in Annex 1.C under Clause 13 will be the Federal Data Protection and Information Commissioner; references to a “Member State” and “EU Member State” will not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and references to “GDPR” in the SCCs will be understood as references to Data Protection Laws of Switzerland.

7.5 TRANSFERS SUBJECT TO UK DATA PROTECTION LAW. If there is a Data Transfer subject to Data Protection Laws of the United Kingdom, then the International Data Transfer Addendum to the SCCs (“UK IDTA”), as issued by the Information Commissioner in the United Kingdom will apply and is incorporated by reference into this DPA. The information needed to complete the Tables to the UK IDTA is set out in the Agreement, including Appendix 1 “Details of Processing” of this DPA.

7.6 EXECUTION. Notwithstanding the fact that the SCCs and/or UK IDTA are incorporated herein by reference without the signature pages of the SCCs actually being signed by the Data Exporter or Data Importer, the parties agree that its respective execution of the Agreement is deemed to constitute its execution of the SCCs and/or the UK IDTA on behalf of the Data Exporter/Data Importer (as applicable).

7.7 ALTERNATIVE MECHANISMS. If an alternative transfer mechanism, such as Binding Corporate Rules, is adopted by NVIDIA, or the Trans-Atlantic Data Privacy Framework (an “Alternative Mechanism”) becomes necessary during the term of the Agreement for the provision of Services, , NVIDIA will notify Customer and the parties will rely on the Alternative Mechanism.

8. ADDITIONAL TERMS FOR PERSONAL DATA SUBJECT TO THE CCPA

In addition to the terms of this DPA, if and to the extent NVIDIA Processes Personal Data that is subject to the California Consumer Privacy Act, as amended (including, without limitation, by the California Privacy Rights Act) hereafter ("CCPA") then the following terms apply. For the purposes of this Section 8, "business", "business purpose", "collects", "consumer", "person", "personal information", "processing", "sell", "service provider" and "share" have their respective meanings as set forth in the CCPA.

(a) NVIDIA will comply with all applicable obligations under the CCPA, including by providing the same level of privacy protection as required by the CCPA;

(b) Customer may take those reasonable and appropriate steps set forth in the DPA and the Agreement to ensure that NVIDIA uses the personal information in a manner consistent with Customer's obligations under the CCPA;

(c) NVIDIA will notify Customer if NVIDIA makes a determination that NVIDIA can no longer meet its obligations under the CCPA;

(d) Customer may, upon notice (including a notice described in (c) immediately above), take those reasonable and appropriate steps set forth in the DPA and the Agreement to stop and remediate unauthorized use of personal information;

(e) NVIDIA will not sell or share any personal information;

(f) NVIDIA will not retain, use, or disclose any personal information for any purpose other than the business purposes specified in the DPA, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purpose specified in the DPA, or as otherwise permitted by the CCPA;

(g) NVIDIA will not retain, use, or disclose personal information for any purpose other than for the the direct business relationship between NVIDIA and Customer;

(i) NVIDIA will not combine any personal information with personal information that is not in the Controller Data that it receives from, or on behalf of, another person or business, or that NVIDIA collects from its own interactions with the consumer outside of the business purposes and the direct business relationship between NVIDIA and Customer, except as permitted by the CCPA; the parties acknowledge and agree that any combining contemplated by the Services is being performed by NVIDIA for the business purposes and the direct business relationship between NVIDIA and Customer; and

(h) Customer may monitor NVIDIA's compliance with this Section in accordance with the audit terms set forth in the DPA.

9. AUDIT

NVIDIA will make available to Customer on request information reasonably necessary to demonstrate compliance with this DPA in the form of certification or audit reports where available. In the absence of certification or audit reports or if compliance with this DPA cannot be reasonably ascertained through certification or audit reports, NVIDIA and Customer will mutually agree, at Customer's cost, on the scope and timing of any additional requests not to exceed once every 12 months. Information shared including any reports are subject to confidentiality requirements.

10. TERMINATION

This DPA will remain in effect until termination of the Agreement. Upon termination of the Agreement, or at Customer's written request, NVIDIA will delete Customer Data in its possession or control within 90 days unless NVIDIA is required by applicable law to retain Customer Data or an alternative agreement is agreed upon. NVIDIA will certify compliance upon Customer's written request.

(v. October 27, 2023)

APPENDIX 1

DETAILS OF PROCESSING

1. Subject matter. The subject matter of the data processing under this DPA is Personal Data included in Customer Data.

2. Duration. As between NVIDIA and Customer, the duration of the data processing under this DPA is the term of the Agreement.

3. Purpose and nature. The purpose and nature of the data processing under this DPA is the provision of the Services.

4. Type of Personal Data. Personal Data included in Customer Data which is uploaded to the Services.

5. Categories of data subjects. The data subjects could include Customer's customers, employees, suppliers, agents, partners, and/or end users.

APPENDIX 2

SECURITY STANDARDS

NVIDIA maintains an information security program based on industry recognized security best practices and standards, and includes the following measures:

1. Organizational Security
    a. NVIDIA's Code of Conduct provides guidance to employees and third parties.
    b. Chief Security Officer or equivalent executive oversees and is accountable for the information security program.
    c. Background checks will be performed on all NVIDIA employees and all contractors at the time of hire subject to applicable law. Background checks may include criminal background check, education history, employment history, and global sanctions.
    d. Security awareness and privacy training will be provided to all employees at the time of hire, and at least annually thereafter.
    e. Risk assessment will be performed as part of risk governance program to regularly identify, assess, and manage security and privacy risk, and evaluate the effectiveness of the information security program.
2. Workstation Security
    a. Technical security measures on NVIDIA managed workstations including device or drive encryption and anti-malware will be implemented and continually maintained.
    b. Asset inventory including hardware and software will be maintained and timely patched against security vulnerabilities.
3. Logical and Physical Access
    a. Access to NVIDIA production systems will be restricted to authorized teams and individuals strictly for administrative, operations, and engineering purposes, and will require multi-factor authentication.
    b. Access will be provisioned in accordance with NVIDIA access management policies, and strictly based upon the principle of least privilege while maintaining appropriate segregation of duties.
    c. Systems will be designed to incorporate authentication and authorization mechanisms, and log and monitor activities.
    d. Data centers will implement physical access and environmental controls including security staff, camera surveillance, badge, and fire detection and suppression systems. Access is limited to appropriate authorized individuals which includes data center administrators, engineers, authorized vendors, and security staff.
    e. Access to resources in the production environment will be controlled through Access Control Lists (ACLs) and network boundary defenses such as firewalls to allow traffic only based on defined rules.
    f. Authorized individuals will be subject to a confidentiality obligation.
4. Data Encryption

a. Customer Data in transit over public networks will be encrypted in accordance with industry standards.

b. Depending on the technology offering(s) Encryption of Customer Data at rest will be implemented by default, or the ability to enable data encryption will be made available to Customer. If encryption at rest is not reasonably available for the technology offering(s), appropriate additional safeguards will be put in place to mitigate the risk of unauthorized access, disclosure, or loss of Customer Data.

5. Vulnerability Management and Monitoring

    a. NVIDIA vulnerability management policies will include identification, assessment, and remediation of vulnerabilities in a timely manner.

    b. Systems and network configurations will be hardened in accordance with industry standards.

    c. Automated and on-demand vulnerability scans of network, infrastructure components, systems, and applications, as well as source code will be performed, and will include one or more of the following:

        i. Static Application Security Testing (SAST)

        ii. Dynamic Application Security Testing (DAST)

        iii. Open-Source Software (OSS) vulnerability scan

        iv. Malware scanning

        v. External end-point vulnerability scanning

6. Logging and Monitoring

    a. Security Operations Center team will monitor central security information and event management system (SIEM) that will include applicable application, system, networking, and infrastructure logs.

7. Change Management

    a. NVIDIA secure development lifecycle will provide consistent guidance for mitigating risks throughout planning, design, coding, verification, release, and operations, and will be periodically updated to adapt to prevailing security risks and trends.

    b. NVIDIA will maintain tools and processes for continuous integration and continuous deployment (CI-CD), where controls will be in place to track, version control, test, and approve changes to meet quality and security objectives.

8. Incident Management

    a. Security operations center will document and maintain incident response plans to timely triage, contain, remediate, and close (report) on potential security incidents.

    b. Incident response plans will include disaster recovery, business continuity and customer notification processes where applicable.

    c. Security incident response team will provide timely information, guidance, and remediation though either targeted communications or by posting a security bulletin.

9. Security Assessment

a. Threat Operations team will perform offensive testing and research, such as penetration testing and attack simulations, at least annually and vulnerabilities identified are remediated timely.

10. Supplier Risk Management

a. Vendor security and privacy assessment will be performed to evaluate controls for material vendors processing, transmitting, and storing Customer Data.

APPENDIX 3

SUB-PROCESSORS

NVIDIA engages with the following Sub-Processors in respect of the Services:

NVIDIA Cloud Service	Sub-Processor
Omniverse Cloud	1. Microsoft - Azure colocation data center hosting and connectivity
DGX Cloud	1. Oracle - Oracle Cloud Infrastructure (OCI) cloud services for hosting and connectivity 2. Microsoft - Azure cloud services for hosting and connectivity 3. Amazon - AWS cloud service provider for supporting cloud services including identity management and access federation