Lenovo NetFilter Data Processor Agreement (DPA)

This Lenovo NetFilter Data Processor Agreement (which addresses both privacy and security requirements) and its annexes, ("**DPA**") form part of the Lenovo Sales Agreement or other written or electronic agreement between Lenovo. and Customer (the "**Agreement**") for the purchase of Lenovo NetFilter services from Lenovo. to reflect the parties' agreement in relation to the Processing of Personal Data.

This DPA supplements any agreement between the parties with respect to the subject matter hereof; and will be effective from the moment that Customer accepts Lenovo NetFilter Terms of Services ("**Effective Date**").

Upon signature of the Agreement and acceptance of the Lenovo NetFilter Terms of Services, this DPA will become legally binding; and you (Customer) are entering into this DPA on behalf of Customer, to the extent required under applicable privacy, security and data protection Laws and Regulations, including applicable education and student privacy and security laws and regulations, in the name and on behalf of its Authorized Affiliates to the extent Lenovo processes Personal Data for which such Authorized Affiliates qualify as the Controller. Customer understands that this DPA is applicable to all users and warrants that it has the necessary powers to enter into this DPA on behalf of such users.

We may update these terms to accommodate new legal requirements or as necessary to reflect operational updates. If you have an active Lenovo NetFilter subscription, we will let you know via email or via in-product notification.

DPA execution:

a) This DPA consists of two parts: the main body of the DPA, and Annexes A, B, C, D and E
b) This DPA has been pre-signed on behalf of Lenovo., including the EU Standard Contractual Clauses in Annex D, as the data importer. (Note: Annex D is generally applicable to only processing activities that may involve the transfer of Personal Data from the European Union, European Economic Area, United Kingdom, and/or other countries with similar adequacy or equivalency standards pertaining to cross-border data transfers).

For the avoidance of doubt, you need to sign this DPA on page 5. If applicable, Annex D will apply by reference.

Data Protection

Definitions: In this Clause, the following terms shall have the following meanings:

a) "**Controller**", "**Processor**", **"Subprocessor",** "**Data Processing**", and "**Processing**" (and "**Process**") shall have the meanings given in EU Data Protection Law and equivalent terms in Applicable Data Protection Law.

b) "**Applicable Data Protection Law**" means all applicable laws, rules, regulations, orders, and all related amendments thereto, in any jurisdiction in which Supplier provides NetFilter Services, including any laws concerning privacy, data security, data protection, data breaches, and confidentiality such as the California Consumer Privacy Act of 2018 ("CCPA") and the California Privacy Rights Act ("CPRA"); the European Union's General Data Protection Regulation 2016/279, as amended, replaced or superseded from time to time ("GDPR"); the United Kingdom's Data Protection Act 2018 as amended; The Brazil Law No. 13.709/18 as amended ("LGPD") and the regulations implemented (or to be implemented); and any such applicable laws, including national, state and/or local education and student privacy laws.

c) **"Personal Data"** is information that relates to an identified or identifiable individual including, but not limited to, students, parents, and school employees.

d) **"Data Subject"** is an individual person who can be identified directly or indirectly including, but not limited to, students, parents, and school employees.

e) **"Customer"** is the Controller. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates.

f) **"Supplier"** means Lenovo, which acts as Processor.

g) **"Data Exporter"** means a party that transfers Personal Data (acting as a Controller) to another Party in accordance with the Agreement.

h) **"Data Importer"** means a party that receives Customer Personal Data (acting as a Processor or Subprocessor) from another Party (Controller) in accordance with this Agreement.

Relationship of the parties: The Controller acknowledges Supplier as a Processor to process the Personal Data that is the subject of Lenovo Sales Agreement, Lenovo NetFilter Terms of Services and EULA with Supplier. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

Purpose limitation: Supplier shall process the Personal Data as a Processor and strictly in accordance with the documented instructions of Controller (the "Permitted Purpose") as documented in Annex A "Processing details", except where otherwise required by any Applicable Data Protection Law. Supplier shall immediately inform Controller if it becomes aware that Controller's Processing instructions infringe Applicable Data Protection Law. In no event shall Supplier process the Personal Data for its own purposes or those of any third-party, including for marketing purposes. For the

avoidance of doubt, Supplier shall not send marketing or otherwise promotional communications to Lenovo NetFilter users leveraging personal data obtained from the use of Lenovo NetFilter. The latter will not prevent any individual from receiving marketing or promotional communications if those originate in the context of standard channels such as Stoneware or Lenovo website and other sales related channels.

International transfers: Supplier may transfer the Personal Data to any country outside of the country from which Personal Data was collected in compliance with applicable Data Protection Laws. For the avoidance of doubt:

a) Personal Data transfers outside of the European Economic Area ("**EEA**") and the United Kingdom are allowed: (i) if the Personal Data transfer is to a recipient in a country that the European Commission, United Kingdom Secretary of State, and/or the United Kingdom's Information Commissioner's Office have decided provides adequate protection for Personal Data; and (ii) to a recipient that has executed standard contractual clauses adopted or approved by the European Commission, United Kingdom Secretary of State, and/or the United Kingdom's Information Commissioner's Office.

   Supplier may transfer the Personal Data outside of Brazil if: (i) the Data transfer is to a recipient in a country that the National Authority has decided provides adequate protection for Personal Data; (ii) to a recipient that has executed standard contractual clauses adopted or approved by the National Authority; or (iii) when the recipient is able to provide and demonstrate the implementation other safeguards in accordance to the Brazilian Data Protection Law and the international transfer is approved by the Controller.

b) Generally, the acceptance of this DPA results in approval by the Customer that Lenovo, Inc. may transfer Personal Data across borders to the extent that Lenovo complies with any applicable Data Protection Laws. In this regard, Annex D "International Data Transfers" applies between Controller and Supplier where relevant.

Confidentiality of Processing: Supplier shall ensure that any person that it authorizes to process the Personal Data (including Supplier's staff, agents and subprocessor) (an "Authorized Person") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Personal Data who is not under such a duty of confidentiality. Supplier shall ensure that all Authorized Persons process the Personal Data only as necessary for the Permitted Purpose. Furthermore, Supplier shall not commercially exploit the Personal Data.

Security: The Processor shall implement appropriate technical and organizational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Personal Data (a "Security Incident"). Annex C contains Lenovo NetFilter Technical and Organizational Measures (TOMs).

Subprocessing: Supplier agrees that any third-party subprocessor it appoints shall be bound to the same standard of data protection provided for by this Agreement; and that Supplier will enter into agreements accordingly with its applicable subprocessors to give appropriate effect to the requirements in this DPA Controller agrees that Supplier may use any subprocessor listed in Annex B.

Notwithstanding this, Controller consents to Supplier engaging new subprocessors (including the replacement of existing ones) to process the Personal Data**, provided that**: (i) Supplier provides at least 30 business days prior notice of the addition or replacement of any subprocessor (including details of the processing it performs or will perform), which may be given by provided details of such addition or replacement to Controller; and (ii) Supplier imposes data protection terms on any subprocessor it appoints that protect the Personal Data to the same standard provided for by this DPA. If Controller refuses to consent to Supplier's appointment of a new third-party subprocessor, which should not be withheld unreasonably, then either Supplier will not appoint the subprocessor or Controller may elect to terminate the Agreement, provided that the Controller has substantial and documented reasons for objection to the change.

Cooperation and Data Subjects' rights: Supplier shall provide reasonable and timely assistance to Controller to enable Controller to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and Personal Data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third-party in connection with the Processing of the Personal Data. For the avoidance of doubt, Data Subject Requests (DSRs) shall be requested by Controller by submitting a formal request in the Stoneware DSR Privacy Webform.

Security incidents: Upon becoming aware of a Security Incident, Supplier shall inform Controller without undue delay and shall provide all such timely information and cooperation as Controller may require to fulfil its Personal Data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Supplier shall further take measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Controller informed of all developments in connection with the Security Incident.

Deletion or return of Data: Upon termination or expiry of the Lenovo Sales Agreement, Supplier shall, upon Controller's request, destroy or return to Controller all Personal Data (including all copies of the Personal Data) in its possession or control (including any Personal Data subcontracted to a third-party for Processing). If Controller does not give further instructions to Supplier, Supplier´s data retention schedule, as laid out in Annex A, will apply. This requirement shall not apply to the extent that Supplier is required by any applicable Data Protection Law to retain some or all of the Personal Data, in which event Supplier shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.

Audit: During the term of this Agreement and for three years after termination or expiration, Supplier shall permit Controller (or its third-party auditors) to audit Supplier's compliance at its own expense and shall make available to Controller information necessary for Controller (or its third-party auditors) to conduct such audit, provided that such audit request is reasonable in scope and that Controller gives it reasonable prior notice of its intention to audit. Controller will not exercise its audit rights more than once in any twelve (12) calendar month period, except if and when required by instruction of a competent data protection authority.

IN WITNESS WHEREOF, Lenovo and Customer have executed this Agreement as of the date written above.

Digital Signer:Kimberly Page
Date:3/16/2023 14:40:03 -04:00

Lenovo
Signature: _____
Print Name: Kimberly Page
Title: Strategic Operations Manager

Custome
Signature: _____
Print Name: _____
Title: _____

ANNEX A – PROCESSING DETAILS

Type of data & data subjects	Retention Period	Nature, purpose, and subject matter
Student Interface related data: • The first name of the student. • The last name of the student. • The e-mail address of the student. • IP Address • Browsing history and Key word Search history	Upon user´s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days.	*Data Access* (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)
School Employee Interface related data: • The first name of the employee. • The last name of the employee. • The e-mail address of the employee. • IP Address • Browsing history and Key word Search history	Upon user´s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days.	*Data Access* (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)
Client Interface related data: • Host Name • Username • IP Address • Web History Searches • Key word searches • Web App Usage • Browser • Device Type • NetFilter App Usage • Browser Data	Upon user´s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days.	*Data Access* (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)
Organization related data • The name of the organization. • Organization Domain	Upon user´s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days.	*Data Storage* (record, host, log, archive or otherwise store Customer Data); *Data Access* (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data);

		Data Analysis (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data).
User data • The first name of the user. • The last name of the user. • The e-mail address of the user. • IP Address • System • Access/Usage/Authorization Data Box • Sensitive/special categories of data: Data logs, web browsing history, machine host name, key word search history.	Upon user´s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days.	*Data Access* (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)
License data (Excludes personal data)	This data is kept as long as necessary to comply with legal obligations, to enforce our agreements, etc. This does not include personal data.	*Data Storage* (record, host, log, archive or otherwise store Customer Data); *Data Access* (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data); *Data Analysis* (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data).

Duration of the Processing
The duration of the processing corresponds to the duration of the Agreement. Data retention policies as described above will apply.
Categories of Data Subjects
Students, Teachers, Organization contacts and Users in general

ANNEX B – SUBPROCESSORS

Name	Data	Storage Location	Purpose
Amazon Web Services	All user data as described in Annex A	US, EU	Cloud service provider for the application infrastructure. All Data is processed by the application.
UDS Web Interface	Identity management data	US, EU	Identity management and authentication authorization.

ANNEX C – TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

Supplier has implemented a comprehensive and written security program with physical, technical, procedural, and administrative controls that reflect prevailing industry standards for the protection and responsible use of Personal Data including, but not limited to, the following controls:

Technical	Scope	Controls
Access	Logins (system & application).	NIST-based password policies (multi-factor authentication for admin-level access and interfaces).
Encryption	Data storage at rest & in transit.	AES 256-GCM (at rest), TLS 1.2 (in transit) ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 (server preferred cipher suites).
Static application security testing	All server and micro-service images, All binary clients and extensions/plugins.	Regular vulnerability scans and monitoring.
Dynamic application security testing	External applications APIs.	Web application scans, Penetration testing (On an AdHoc basis as scheduled by SSRB).
CIS benchmark hardening	Cloud platform provider, Server instances.	Cloud CIS compliance checks, Cloud security monitoring, Regular CIS L2 server benchmark assessments.
Software compositional analysis	3rd party opensource dependencies.	Conduct regular vulnerability audits, repository monitoring.
Infrastructure assessment	Cloud platform provider.	Regular reviews of all software-defined networks (SDNs) (identify network segmentation, firewall configuration, and resource access misconfigurations).
Web application firewall (WAF)	Production web applications.	WAF protection (core rules for common attacks).
Static code analysis owned by Netsweeper	Proprietary code.	Regular code analysis is conducted using a commercial tool, will be done with each code release.
Log collection	Cloud platform provider, Application.	Cloud platform API transactions (logs older than one year are purged, accessible through Datadog and available to internal users with Lenovo Active Directory Integration for SAML 2.0 auth), WAF logging for edge detection (logs reside only within the instance, accessible by engineering),

		Subprocessors, see Annex B, for application purposes.
Infrastructure as code	Cloud platform provider.	Infrastructure as code is used to automate infrastructure deployments and improve the immutability, misconfiguration of infrastructure.

Organizational	Scope	Controls
Incident (including data breach) response	Security events related to products in production.	Product incident response plan in accordance with NIST 800-61 and Lenovo's internal Product Security Incident Response Team (PSIRT) processes.
Trusted providers list	All subprocessors that directly integrate with products in production.	Standard security assessments of integrated providers, DPAs for Personal Data processing providers.
Vulnerability management	Server OSes, Docker containers, Clients, Products in production.	A program that employs various tools to aid in identifying vulnerabilities across all compute systems.
Software Security Review Board (SSRB) And Cloud Security Review Board (CSRB)	Products in production.	SSRB reviews are conducted during every release. CSRB reviews are conducted during every change in architecture. During reviews all technical and organizational measures are assessed for the product in question.
Data retention policy	Personal identifiable information, Application data, Products in production.	Upon user's request for deletion, or after one year of not having an active license or trial, or after any arbitrary time should the business no longer require the data and the data is void of security implication.
Security and privacy awareness	All employees (Privacy Basics and Security Essentials courses)	Regular trainings for specialized IT and product teams on advanced security topics, such as OWASP Top 10.
Continuous security	Products in production.	Regular application of Technical Measures.
Opensource compliance reviews.	Products in production.	Assessments conducted to ensure proper licensing and attributions are provided in distributed software.

Disaster Recovery	Products in production	Following NIST-800-34 as a guide to maximize RTO and RPO.
Backup policy	Databases, Code, Logs.	For Database backup / restore, encrypted backup (encrypted at rest) is used which is also highly available on multiple Availability Zone and can be restored within 30 mins. Previous 7-day backup is retained, and they are rotated. Manual snapshot if taken, can be stored indefinitely (1 year or more). Additionally automated (UDS) solution which runs cron job to encrypt and back up databases which retains it for a period of 7 days on rotation is also available. Application source code which includes 'Infrastructure as Code' (as well as DB creation) is on the UDS enterprise version are backed up indefinitely. Production logs are available on DataDog for 30 days. UDS is still in the process of extending these logs to 12 months on a cold archive.

ANNEX D – INTERNATIONAL DATA TRANSFER AGREEMENT

This Annex sets out the data protection requirements (including requirements under Applicable Privacy Laws) that apply: (i) to the Data Exporter (Controller) when it transfers Personal Data to the Data Importer (Lenovo.), its affiliates and/or its Subprocessors, for Data Processing; and (ii) to the Data Importer when it receives Personal Data from a Data Exporter for Data Processing.

The Data Importer warrants and undertakes that at all times it will:

a) Process the Transferred Data in accordance with Applicable Privacy Laws and will provide reasonable and timely assistance to the Data Exporter as needed to help the Data Exporter comply with its obligations under Applicable Privacy Laws; and

b) not knowingly perform its obligations under this Agreement in such a way as to cause the Data Exporter to breach any of its obligations under Applicable Privacy Laws.

1. European Economic Area (EEA)

If Supplier's services are provided to Controller within the European Economic Area ("EEA") or such other jurisdiction subject to EU Data Protection Law, the following provisions shall apply:

(A) "EU Data Protection Law" means (a) 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) (the "GDPR"); (b) the EU e-Privacy Directive (Directive 2002/58/EC); and (c) any and all applicable national data protection laws.

(B) Supplier shall promptly inform Controller (a) of any requirement under EU Data Protection Law that would require Processing Personal Data in any way other than per Controller's instructions, or (b) if, in Supplier's opinion, Controller's instructions may infringe or violate any applicable EU Data Protection Law.

(C) ***Data Transfers:*** If Supplier or its Subcontractors are located outside the EEA, Supplier and Controller hereby execute the controller to processor standard contractual clauses as set out in MODULE TWO in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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 amended or superseded from time to time (the "C2P Standard Contractual Clauses") and hereby incorporate them into this Addendum by reference. The parties acknowledge and agree that:

a. Supplier and Controller shall each comply with their respective obligations in the C2P Standard Contractual Clauses;

b. If there is any conflict or inconsistency between the C2P Standard Contractual Clauses and this Addendum or the base agreement, the C2P Standard Contractual Clauses shall control to the extent of the conflict; and

c. The information in the following tables is hereby incorporated into the C2P Standard Contractual Clauses between the Parties:

Information to be incorporated into the
C2P Standard Contractual Clauses between Controller and Supplier:

Clause 9. Use of sub-processors	Option 2 GENERAL WRITTEN AUTHORISATION is selected. Data importer shall provide information at least 30 days in advance as per Clause "Subprocessing"
Clause 17. Governing law	These Clauses shall be construed in accordance with the governing law set forth in the Parties' base agreement unless that governing law is not that of an EU Member State that allows for third-party beneficiary rights. In such event, the Parties agree that these Clauses shall be governed by the law of IRELAND.
Clause 18 (b). Choice of forum and jurisdiction	The Parties agree that any dispute arising from these Clauses shall be resolved by the courts of IRELAND.

Information to be incorporated into Annex 1, Part A of the C2P Standard Contractual Clauses:

Data Exporter's Name	Controller, and any of its commonly owned or controlled affiliates
Data Exporter's Address	To be completed by data exporter
Data Exporter´s contact person´s name, position and contact details	To be completed by data exporter
Data Exporter´s activities relevant to the data transferred under these Clauses	To be completed by data exporter
Data Exporter´s signature and date	To be completed by data exporter
Data Exporter´s role	Controller
Data Importer's name	Supplier (Lenovo) and its Subcontractors
Data Importer´s address	3400 E Coliseum Blvd, #310, Fort Wayne, IN 46805 United States of America
Data Importer´s contact person´s name, position and contact details	Kimberly Page, Strategic Operations Manager privacy@lanschool.com
Data Importer´s activities relevant to the data transferred under these Clauses	As set out in Part B of Annex 1
Data Importer´s signature and date	To be completed by data importer
Data Importer's Role	Processor

Information to be incorporated into Annex 1, Parts B and C of the C2P Standard Contractual Clauses:

Categories of data subjects	As set out in Annex A above
Categories of personal data	As set out in Annex A above
Sensitive data	As set out in Annex A above
Frequency of the Transfer	Ongoing frequency, as long as LSA license is active
Nature of the processing	As set out in Annex A above
Purpose of the processing	As set out in Annex A above
Period for which personal data will be retained	As set out in Annex A above
Subject matter, nature and duration of the processing carried out by subprocessors	As set out in Annex B above
Competent Supervisory Authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 ty	The supervisory authority that will act as competent supervisory authority will be that of the EU member State where Data Exporter is established in the EU. If Data Exporter (I.e., contracting legal entity) is not established in EU, then the Competent Supervisory Authority will be such of the EU Member State in which the Data Exporter´s EU representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established. If the Data Exporter is not established in the EU but does not need to appoint an EU representative, then the Competent Supervisory Authority will be that of the EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

Information to be incorporated into Annex 2 of the C2P Standard Contractual Clauses:

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.	As set out in Annex C above

Information to be incorporated into Annex 3 of the C2P Standard Contract Clauses:

List of authorized sub-processors	As set out in Annex B above

2. United Kingdom (UK)

If Supplier's services are provided to Controller within the United Kingdom, or the nature of the Personal Data triggers the application of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and the Data Protection Act 2018 (the "DPA 2018"), the following additional provisions shall apply:

(A) Transfers of Personal Data to a recipient in a country considered by the UK's Secretary of State, to provide adequate protection for Personal Data (an "Adequacy Decision") will be permitted under the Agreement(s) without the need for approved UK Standard Contractual Clauses.
(B) EEA countries shall be deemed to be subject to an Adequacy Decision for the purpose of transfers of Personal Data from the UK to the EEA.
(C) In the absence of an Adequacy Decision, Controller and Supplier agree to execute approved UK International data transfer addendum to the European Commission's standard contractual clauses for international data transfers (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

Part 1: Tables / Table 1: Parties

Information to be incorporated into "Part 1: Tables" of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses:		
Start date	As per the above	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name, main address (if a company registered address): As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D Official registration number (if any) (company number or similar identifier): As per customer identified under the Sales Agreement	Full legal name, main address (if a company registered address): As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D Official registration number (if any) (company number or similar identifier): 35-2097171 registered in State of Indiana
Key Contact	Full Name (optional), job title, contact details including email: As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D	Full Name (optional), job title, contact details including email: As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	See Annex D, Art. 1 above

Table 3: Appendix Information

Annex 1A: List of Parties As set out in in the Art. 1. European Economic Area (EEA) in the Annex D
Annex 1B: Description of Transfer: As set out in Annex A above
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Description of Transfer: As set out in Annex C above
Annex III: List of Sub processors (Modules 2 and 3 only): Description of Transfer: As set out in Annex B above

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: x Importer ☐ Exporter ☐ neither Party

Information to be incorporated into "Part 2: Mandatory Clauses" of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses:
Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

3. Switzerland

Until Swiss relevant authorities release Swiss Model Clauses, C2P Model Clauses as executed under section 1 "European Economic Area (EEA)" above apply by reference. In the event that the European Commission or the Swiss government agrees a successor solution to the Swiss-US Privacy Shield, then provisions under section 2 "United Kingdom (UK)" above apply by reference.

4. Brazil

Until Brazil relevant authorities release equivalent Brazil Model Clauses, C2P Model Clauses as executed under section 1 "European Economic Area (EEA)" above apply by reference.

5. South Africa

If Supplier's services are provided to Controller within South Africa or such other jurisdiction subject to the Protection of Personal Information Act (POPIA), the following additional provisions shall apply:

(A) Data Subject means a natural person who can be identified by reference to a name, unique number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person as well as an identifiable juristic person or legal entity.

ANNEX E – ADDITIONAL PROVISIONS

1. California Consumer Privacy Act ("CCPA").

Lenovo is a Business. Additionally, Supplier is Customer´s Service Provider and will process Personal Data on behalf of Customer.

a. Supplier shall not sell the Personal Data or Proprietary Information. "Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating the information for monetary or other valuable consideration.

b. Supplier shall not retain, use, or disclose the Personal Data: (a) for any purpose other than for the specific purpose of performing the services set forth in the Agreement for Lenovo or as otherwise permitted by the CCPA and its implementing regulations, (b) for a commercial purpose other than providing the services specified in the contract with the business, or (c) outside the direct business relationship between the person and Lenovo

c. This DPA shall serve as Supplier's certification that Supplier understands the CCPA requirements applicable to businesses and service providers, including the restrictions in Cal. Civ. Code § 1798.140(w)(2)(A), and will comply with them.