NETAPP SUPPLIER DATA PROCESSING ADDENDUM

RECITAL

This Data Processing Addendum ("**Addendum**") is entered into to ensure adequate privacy and security safeguards when Personal Data is exported from one Party and imported and Processed by another Party, as authorized by the data exporter and in accordance with applicable Data Protection Laws.

By signing this Addendum, each Party agrees to the data protection requirements included herein on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates.

SCOPE AND APPLICATION

This Addendum will apply to all products and services provided by a Supplier to or on behalf of NetApp pursuant to the Agreement(s).

The scope of this Addendum applies to all Personal Data:

- Sent by or on behalf of NetApp (data exporter) to the Supplier (data importer),
- Accessed by the Supplier and its Affiliates, on the authority of the NetApp,
- Otherwise received by the data processor, and its Affiliates, for Processing on NetApp's behalf.

NetApp

SUPPLIER DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is made as of the date of last signature below (the "**Addendum Effective Date**") by and between **NetApp, Inc.**, a Delaware corporation with its address at 3060 Olsen Drive, San Jose, CA 95128 and its Affiliates (collectively "**NetApp**") and **_____, a [INSERT STATE/COUNTRY OF INCORPORATION OR BUSINESS FORMATION][INSERT TYPE OF BUSINESS ENTITY, E. G. , CORPORATION, LIMITED LIABILITY COMPANY, ETC.]** with its address at **[INSERT SUPPLIER ADDRESS AS LISTED ON CORRESPONDING MASTER]** ("**Supplier**"), pursuant to that certain **[INSERT TITLE OF MASTER AGREEMENT]** between the Parties dated as of **INSERT EFFECTIVE DATE OF MASTER** (the "**Agreement**") to which this Addendum is hereby incorporated by reference.

This Addendum consists of:

- the terms and conditions below; and
- Appendix 1
  - Annex 1, Description of Transfer;
  - Annex 2, Security Standards; and
  - Annex 3, List of Subprocessors.

Upon execution of this Addendum, the entire Agreement shall consist of:

- this Addendum;
- the Agreement, as defined above;
- any exhibits expressly incorporated into the Agreement; and
- any other terms expressly adopted or incorporated by reference into the Agreement.

All other terms and conditions from the Agreement remain intact and in full force and effect.

IN WITNESS THEREOF, the duly authorized representatives of the parties hereto have caused this Addendum to be duly executed.

SUPPLIER NAME		**NetApp, Inc.**	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

NetApp

1. Definitions.

All capitalized terms not defined herein will have the meaning set forth in the applicable Agreement. The following terms have the following meanings:

1.1. **"Affiliate"** shall have the meaning ascribed to it under the Agreement, or, where the Agreement does not contain a definition, "Affiliate" means, in relation to either Party, any entity: (a) which is owned more than 50% by that Party; or (b) over which that Party exercises management control; or (c) which is under common control with that Party; or (d) which owns more than 50% of that Party's voting securities.

1.2. **"Appendix 1"** refers to, collectively, Annex 1, Annex 2, and Annex 3 as attached hereto and fully incorporated herein.

1.3. **"Data Protection Laws"** means all applicable laws and regulations governing the Processing of Personal Data under the Agreement, including relevant local, national and international data privacy and protection laws and regulations.

1.4. **"Data Subject"** means any identified or identifiable individual whose Personal Data is Processed in respect of the provision of Services under the Agreement.

1.5. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016.

1.6. **"NetApp Data"** means any information owned or processed by NetApp, in any form, format or media (including paper, electronic and other records), which Supplier has access to, obtains, uses, maintains or otherwise handles in connection with the performance of the Agreement, including partial copies thereof.

1.7. **"Personal Data"** means any information relating to an identified or identifiable living individual or any other information defined as 'personal data' or 'personal information' under applicable Data Protection Laws.

1.8. "**Process**" or "**Processing**" means any operation which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.9. "**Security Incident**" means any accidental or unauthorized access, acquisition, use, modification, disclosure, loss, destruction or, or damage to NetApp Data, or any other unauthorized Processing of NetApp Data.

1.10. **"Sensitive Data"** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation.

1.11. **"Standard Contractual Clauses"** means (i) where the GDPR applies, the EU Standard Contractual Clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**"); and (ii) where the UK GDPR applies, the UK Data Transfer Addendum ("**UK DTA**") issued by the Commissioner under S119A(1) Data Protection Act 2018, in each case as may be amended, superseded or replaced from time to time.

1.12. "**Third Country**" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for Personal Data.

1.13. "**Transfer**" means the access by, transfer or delivery to, or disclosure of Personal Data to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction from where the Personal Data originated.

1.14. "**UK GDPR**" means the GDPR as incorporated into United Kingdom domestic law pursuant to Section 3 of the European Union (Withdrawal) Act 2018.

2. Limitations on Use

2.1. Supplier will Process Personal Data as specified in this Addendum and in the applicable Agreement. Supplier acknowledges that while providing Services under the Agreement, Supplier acts as a data processor or subprocessor to NetApp and may process Personal Data of Data Subjects of the (1) European Economic Area outside of the EEA and Switzerland (together, for the purposes of this Agreement, the "**EEA**"); and (2) United Kingdom ("**UK**") outside of the UK. Supplier will, as part of its Services, comply with its obligations in this Addendum. The details of Processing are described in the Description of Transfer in Annex 1 to Appendix 1 of this Addendum.

2.2. Supplier is prohibited from using, disclosing, sharing or otherwise selling Personal Data, except as expressly permitted in the Agreement and this Addendum. Supplier shall Process Personal Data in accordance with Data Protection Laws, and applicable policies and standards specifically identified in this Addendum and in the Agreement.

3. Confidentiality

Supplier shall ensure that persons authorized by Supplier to Process NetApp Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Data Security

4.1. **Information Security Program.** Supplier must implement, maintain, monitor, and, where necessary, update a comprehensive written information security program that contains appropriate technical and organizational measures to protect NetApp Data against threats or hazards to its security, confidentiality, or integrity (such as unauthorized access, collection, use, copying, modification, disposal or disclosure, loss, destruction), in particular where the Personal Data is transferred over a network, and against all other unlawful forms of Processing (the "**Information Security Program**"). The technical and organizational measures implemented by Supplier must ensure a level of security reasonably appropriate to the risk of the processing. At a minimum, such technical and organizational measures must include without limitation the measures set forth in the Security Standards in Appendix 2 of this Addendum. Without limiting the foregoing:

A. Supplier will maintain and enforce its Information Security Program at each location from which Supplier provides services to NetApp. In addition, Supplier will ensure that its Information Security Program covers all networks, systems, servers, computers, notebooks, laptops, tablets, mobile phones, and other devices and media that process, host or store NetApp Data or provide access to NetApp systems.

B. Supplier will review and, as appropriate, revise its Information Security Program at least annually or whenever there is a material change in Supplier's business practices that may affect the security, confidentiality or integrity of NetApp Data.

4.2. **Security Incident.** Supplier will notify NetApp in writing without undue delay and as soon as reasonably possible (and in any event within forty-eight (48) hours) whenever Supplier reasonably believes that there has been, or suspects there may have been, any Security Incident. After providing notice, Supplier will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of the Personal Data, and keep NetApp informed of the status of the Security Incident and all related matters. Supplier further agrees, at the cost of Supplier, to provide reasonable assistance and cooperation requested by NetApp and/or NetApp's designated representatives, in the furtherance of any correction, remediation, or investigation of any Security Incident and/or the mitigation of any potential damage, including any notification that NetApp may determine appropriate to send to affected individuals, regulators or third parties, and/or the provision of any credit reporting service that NetApp deems appropriate to provide to affected Data Subjects. Unless required by law applicable to Supplier, Supplier will not notify any individual or any third party other than law enforcement of any potential Security Incident involving Personal

Data without first obtaining written permission of NetApp. In the event the Supplier does not remedy a Security Incident to the reasonable satisfaction of NetApp, then NetApp has the right to terminate the Agreement.

5. **Disclosure.** Supplier may not disclose or transfer any Personal Data to, or allow access to Personal Data (each, a "**Disclosure**"), by any third party (including its Affiliates or subcontractors) or a Third Country without NetApp's express prior written consent; provided, however, that Supplier may Disclose Personal Data to its Affiliates and subcontractors for purposes of providing the Services to NetApp, subject to the following conditions, unless otherwise stated in Appendix 1: (a) Supplier will maintain a list of the Affiliates and subcontractors to which it makes such Disclosures and will provide this list to NetApp upon NetApp's request; (b) Supplier will provide NetApp at least 30 days' prior notice of the addition of any Affiliate or subcontractor to this list and the opportunity to object to such addition(s); and (c) if NetApp makes an objection on reasonable grounds and Supplier is unable to modify the Services to prevent Disclosure of Personal Data to the additional Affiliate or subcontractor, NetApp will have the right to terminate the relevant Processing. Supplier will, prior to any Disclosure, enter into an agreement with the third party that is at least as restrictive as this Agreement. That agreement will be provided to NetApp promptly upon request. Supplier will ensure that any such subcontractor can comply with those obligations and will be fully liable for any acts or omissions of the subcontractor with respect to the Personal Data to the same extent as if the acts or omissions were those of Supplier.
6. **Disclosure Requests**. If Supplier receives any order, demand, warrant, or any other document requesting or purporting to compel the production of Personal Data ("**Disclosure Request**"), Supplier will immediately notify NetApp (except to the extent otherwise required by laws applicable to Supplier). If Supplier reasonably determines that a Disclosure Request is not legally valid and binding, Supplier will not respond. If Supplier reasonably determines a Disclosure Request is legally valid and binding, Supplier will provide NetApp at least 72 hours' notice prior to the required disclosure, so that NetApp may, at its own expense, exercise such rights as it may have under applicable law to prevent or limit such disclosure. Notwithstanding the foregoing, Supplier will exercise commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of Personal Data and will cooperate with NetApp with respect to any action taken with respect to such request, complaint, order or other document, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Personal Data.
7. **Requests or Complaints from Data Subjects.** Supplier will promptly notify NetApp in writing, and in any case within 48 hours of receipt, if Supplier receives: (i) any requests from a Data Subject with respect to NetApp Data, including but not limited to opt-out requests, requests for access and/or rectification, blocking, erasure, requests for data portability, or other similar requests; or (ii) any complaint relating to the Processing by Supplier of NetApp Data, including allegations that such Processing infringes on a Data Subject's rights. Supplier will cooperate with NetApp with respect to any action taken relating to such request or complaint and will seek to implement appropriate technical and organizational measures to assist NetApp in addressing those requests. Supplier will not respond to any such requests or complaints unless expressly authorized to do so by NetApp.
8. **Regulatory Investigations.** Supplier will promptly notify NetApp in writing, and in any case within 48 hours of receipt, if Supplier receives any request, query, or investigation of any regulator relating to NetApp Data. At NetApp's request, Supplier will assist and support NetApp in the event of an investigation by any regulator, including a data protection regulator, or similar authority, if and to the extent that such investigation relates to Personal Data handled by Supplier on behalf of NetApp in accordance with this Agreement. Such assistance will be at NetApp's sole expense, except where investigation was required due to Supplier's acts or omissions, in which case such assistance will be at Supplier's sole expense.
9. **Cooperation and Assistance.** Supplier will provide relevant information and assistance requested by NetApp to demonstrate Supplier's compliance with its obligations under this Addendum and assist NetApp in meeting its obligations under applicable Data Protection Laws regarding: (i) registration and notification;

(ii) accountability; (iii) ensuring the security of the Personal Data; and (iv) the carrying out of privacy and data protection impact assessments and related consultations of data protection authorities. Supplier will inform NetApp if Supplier believes that any instructions of NetApp regarding the Processing of Personal Data would violate applicable law.

10. **Audit.** NetApp may provide to Supplier a security assessment questionnaire related to the Services, which Supplier will accurately and promptly complete. That questionnaire may include questions seeking verification of compliance with the terms and conditions of this Addendum. Upon request, Supplier will also supply a copy of its most recent third-party assessment, such as an ISO 27001, SSAE 16 SOC 2, ISAE 3402 or similar assessment, if Supplier has had such an assessment performed. If, after the original security questionnaire assessment, NetApp determines that further assessment is warranted, NetApp may (i) itself or through a third party auditor, conduct audits (including inspections) during the term of the Agreement to assess Supplier's compliance with the terms of this Addendum; and (ii) request, no more than annually and with 30 days' prior written notice, an assessment related to the Services provided with a scope to be mutually agreed. During its review, NetApp may examine policies, procedures and other materials related to specific Services performed, to the extent that such review does not compromise confidentiality obligations to any other customers of Supplier.

11. **Adverse Changes.** Supplier will notify NetApp promptly if Supplier: (i) has reason to believe that it is unable to comply with any of its obligations under this Addendum and it cannot implement a remedy within a reasonable time; or (ii) becomes aware of any circumstances or change in applicable law that is likely to prevent it from fulfilling its obligations under this Addendum. If Supplier provides such notice, NetApp will have the right to temporarily suspend the relevant Processing until such time that the Processing is adjusted in such a manner that the noncompliance is remedied. To the extent such adjustment is not possible, NetApp will have the right to terminate any or all Agreements, without liability to NetApp.

12. **Data Transfers.**

12.1. **Transfers from the EEA**. Where NetApp or a NetApp Affiliate in the EEA Transfers Personal Data which is subject to the GDPR to Supplier or an approved subcontractor that is located in a Third Country, the parties agree that such transfers will be governed by the EU SCCs, in addition to this Addendum.

12.2. **Transfers from the UK.** Where NetApp or a NetApp Affiliate in the UK Transfers Personal Data which is subject to the UK GDPR to Supplier or an approved subcontractor that is located in a Third Country, the parties agree that such transfers will be governed by the UK Addendum to the EU SCCs, in addition to this Addendum.

12.3. **Transfers from non-EEA Countries.** When NetApp or a NetApp Affiliate in a non-EEA country in which the competent data protection authority has approved the use of the EU SCCs for restricted Transfers of Personal Data from the relevant country to Supplier or its subcontractors located outside such non-EEA country, the parties agree that such Transfer will be governed by the EU SCCs, in addition to this Addendum.

12.4. **Transfers from Switzerland.** Where NetApp Data is transferred from Switzerland, the following provisions apply: (i) general and specific references in the EU SCCs to GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws; (ii) in respect of data transfers governed by Swiss Data Protection Laws, the EU SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity; (iii) where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws; and (iv) for Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

13. **NetApp Data subject to the CCPA/CPRA.**

As used in this Section 13, "**Commercial Purpose**", "**Consumer**", "**Personal Information**", "**Sell**", and "**Service Provider**" have the meanings assigned to them in the CCPA/CPRA.

13.1. If NetApp Data comprises Personal Data subject to the CCPA/CPRA ("**CCPA/CPRA Covered Data**"), Supplier is the Service Provider and, consistent with the requirements of the CCPA/CPRA, Supplier shall not (a) Sell the CCPA/CPRA Covered Data or (b) retain, use or disclose the CCPA/CPRA Covered Data: (i) for any purpose, including any Commercial Purpose, other than the specific purpose of providing and supporting the product or service or (ii) outside of the Parties' direct business relationship, or (iii) for any purpose other than legally permitted business purposes under the CCPA/CPRA and its regulations.

13.2. NetApp is the customer and is responsible for responding to Consumer requests in relation to CCPA/CPRA Covered Data (each, a "**Consumer Request**"). If Supplier receives a Consumer Request, then, to the extent legally permissible, Supplier will advise the Consumer to submit the Consumer Request to the customer. To the extent the customer is unable through its use of the product or service to address a particular Consumer Request, Supplier will, upon request and considering the nature of the CCPA/CPRA Covered Data, provide reasonable assistance in addressing the Consumer Request (provided that Supplier is legally permitted to do so). The customer is responsible for verifying Consumer Requests in accordance with the CCPA/CPRA.

14. **NetApp Data subject to LGDP.** If NetApp Data comprises Personal Data subject to the LGPD ("**LGPD Covered Data**"), then Personal Data, as the term is used in this Addendum shall be deemed to include LGPD Covered Data.

15. **NetApp Data subject to global data protection laws.** Parties agree to comply with applicable local, national and international data privacy and protection laws and regulations.

16. **Third-Party Beneficiaries.** The Parties agree that NetApp's Affiliates are intended third party beneficiaries of this Addendum and that this Addendum is intended to inure to the benefit of such Affiliates. Without limiting the foregoing, NetApp Affiliates will be entitled to enforce the terms of this Addendum as if each was a signatory. NetApp also may enforce the privacy and data security provisions on behalf of NetApp Affiliates (instead of NetApp Affiliate(s) separately bringing a cause of action against Supplier). Supplier will be entitled to rely solely on NetApp's instructions relating to NetApp Data.

17. **Duration and Termination**

17.1. Supplier's obligations under this Addendum will continue as long as Supplier continues to have access to, is in possession of, or requires NetApp Data, even if any applicable agreement between the Parties has expired or been terminated.

17.2. Upon termination or expiration of the Agreement, or earlier upon NetApp's request, Supplier will immediately return all original and copies of Personal Data to NetApp or, upon NetApp's request, destroy any or all Personal Data in Supplier's possession, power or control. If Supplier has such a legal obligation to retain Personal Data beyond the period otherwise specified by this Section, Supplier will notify NetApp in writing of that obligation, to the extent permitted by applicable law, and will return or destroy the NetApp Data in accordance with this Section as soon as possible after that legally required retention period has ended. If Supplier disposes of any paper, electronic or other record containing Personal Data, Supplier will do so by taking all reasonable steps (based on the sensitivity of Personal Data) to destroy Personal Data by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying Personal Data in such records to make it unreadable, non-reconstructable and indecipherable. Supplier will provide a written certification that Personal Data has been returned or securely destroyed in accordance with this Addendum.

18. Miscellaneous

18.1. **Counterparts.** The parties may execute this Addendum in any number of counterparts. Each counterpart will be deemed an original and all counterparts will constitute one addendum binding on both parties. Facsimile and electronic signatures will be considered binding for all purposes.

18.2. **Governing Law.** The provisions in this Addendum relating to data protection aspects for the processing of Personal Data, excluding Appendix 1, shall be governed by the laws of the State of California.

18.3. **Changes to Legislation.** Unless the context dictates otherwise, any reference in this Addendum to a law or regulation of any jurisdiction of any country shall include any replacement to, addition to, or amendment of, such law or regulation from time to time.

18.4. **No Further Amendment.** Except as modified by this Addendum, the Agreement remains unmodified and in full force and effect.

18.5. **Conflict.** In the case of any inconsistency between this Addendum and the Agreement, the inconsistency shall be resolved so as to provide an adequate level of data protection for the personal data under applicable law. Furthermore, pursuant to Clause 2 of the Standard Contractual Clauses, any language in this Addendum which provides additional safeguards to NetApp over the NetApp Data and Personal Data, is intended to supersede and control.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

APPENDIX 1

Annex 1: DESCRIPTION OF PROCESSING AND TRANSFER OF PERSONAL DATA

This Annex 1 describes the Processing of Personal Data for the EU SCCs and applicable Data Protection Laws.

I. LIST OF PARTIES

A. The **Data Exporter** is NetApp.

NetApp Data Protection Legal Team
3060 Olsen Drive, San Jose, CA 95128
dataprotection@netapp.com

B. **Data Importer** is Supplier and its subprocessors (as set forth in Annex 3) that provide services and/or support to NetApp.

SUPPLIER TO PROVIDE CONTACT INFORMATION FOR DPO OR DATA PRIVACY TEAM

II. DESCRIPTION OF TRANSFER

A. The Parties agree that any transfer of NetApp Data from the EEA to a Third Country shall be subject to the EU SCCs, or other permitted transfer mechanisms as allowed per the GDPR, which are incorporated by reference and shall form part of this Addendum.

With respect to the EU SCCs, they shall be deemed completed as follows:

1. Module Two (Controller to Processor) will apply, where the data exporter is NetApp and the data importer is Supplier;
2. In Clause 7 (Docking), the optional docking clause will apply;
3. In Clause 9 (Use of subprocessors), option 2 "General Written Authorization" for subprocessors shall apply and the time period for prior notice shall be as set out in section 5(b) of this Addendum;
4. In Clause 11 (Redress), the optional language shall not apply;
5. In Clause 13 (Supervision), the competent supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards to the data transfer, is indicated in Annex 1 Part III and shall act as competent supervisory authority;
6. In Clause 17 (Governing Law), the EU SCCs shall be governed by the laws of Ireland;
7. In Clause 18(b) (Choice of Forum and Jurisdiction), the parties agree that disputes shall be resolved before the courts of Ireland; and
8. Module Three (Processor to Processor) will apply, where NetApp is the data importer and the data exporter is the Supplier.

B. Where NetApp Data is transferred from the UK to a Third Country, the parties agree that the UK Addendum to the EU SCCs shall be deemed executed by the parties.

The information required by the UK Addendum is as follows:

1. for Table 1 of Part One of the UK Addendum, it shall be deemed completed with the information set forth in Appendix 1, Annex 1 and the Agreement;

2. for Table 2 of Part One of the UK Addendum, it shall be deemed completed with the information set forth in Appendix 1, Annex 1;

3. for Table 3 of Part One of the UK Addendum, it shall be deemed completed with the information set forth in Appendix 1, Annexes 1-3; and

4. for Table 4 of Part One of the UK Addendum, the boxes for “Importer” and “Exporter” are selected.

C. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects:

- ☐ Prospective NetApp customers
- ☐ NetApp Customers
- ☐ NetApp Business Partners
- ☐ NetApp Vendors
- ☐ NetApp Employees, agents, contractors Other individuals providing Personal
- ☐ Data to NetApp, thereafter, transmitted to, made available to, accessed or otherwise processed by the Supplier

D. Categories of Personal Data

The Personal Data transferred may include, but not be limited to, some or all of the following categories of Personal Data and will be further specified in a SOW or other ordering document:

Category	Description
Personal identification	Name, date of birth
Authentication data	Password, security question
Contact information	Address, email, business contact information
Unique identifiers and signatures	Social Security number, bank account number, signature
Financial and insurance information	Bank account name and number, credit card name and number, creditworthiness
Commercial Information	History of purchases, subscription information, payment history
Location data	Cell ID, geo-location network data, location by start call/end of the call, location data derived from use of wifi access points
Profiling	Observance of criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences
Internet activity	Browsing history, search history, reading, television viewing, radio listening activities
Device identification	IMEI-number, SIM card number, MAC address

Citizenship information	Citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit
HR and recruitment data	Employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations
Education data	Education history, current education, grades and results, highest degree achieved, learning disability
Miscellaneous/Other	Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority Any other personal data as defined in Article 4 the GDPR

E. Sensitive Personal Data (if applicable)

The transmission of Sensitive Personal Data may include special categories of personal data, or sensitive data. Supplier has adopted the relevant security measures are described in Annex 2 to ensure the appropriate level of security.

F. Frequency of the transfer

Unless otherwise specifically outlined in an applicable statement of work or order form, transfers of personal data will occur on a continuous basis for the duration of the Agreement.

G. Nature of the processing

The data exporter shall provide the data importer with personal data obtained through the Services.

H. Purposes of the data transfer and further processing

The purpose of the data transfer and processing is to allow Supplier's provision of online services, professional services, and/or consumer services or products, as further described in an applicable SOW or ordering document.

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

Supplier will delete all personal data immediately after the business purposes for which the personal data was collected or transferred have been fulfilled, or upon NetApp's written request, whichever occurs earlier.

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

The transfer of personal data will occur on a continuous basis for the duration of the Agreement. Supplier's subcontractors and/or Affiliates may be subprocessors to support Supplier's services as outlined in an applicable SOW or other ordering document, which is also the purpose of the data transfer for further processing, provided that the permission for Supplier to use such subcontractor or Affiliate is compliant with Annex 3 of this Appendix 1.

III. Competent Supervisory Authority

Where NetApp is the data exporter, the supervisory authority shall be the Data Protection Commission of Ireland.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Annex 2: SECURITY STANDARDS

TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Supplier has implemented and will maintain the security measures identified below.

PHYSICAL ACCESS CONTROLS	
Measures taken to restrict inappropriate access to personal data, and transfer of media and equipment on which personal data is stored.	Limited physical access to facilities (e.g. doors locked electronically or physically)
	Access control systems (e.g. biometric security, access card security)
	Presence of security personnel (e.g. security at front desk)
	Emergency and contingency plans for facilities
	Personnel and subcontractors must obtain authorization prior to storing personal data on portable devices, remotely accessing personal data, or processing personal data outside of approved facilities
	Additional physical security measures to protect IT systems (e.g., partitioned server room) (Please specify): *Additional swipe system on server room door.*
TECHNICAL ACCESS CONTROLS	
Measures taken to restrict access to its data-processing systems.	Information systems require individual users to log in using unique usernames
	Information systems require use of strong/complex passwords and require mandatory password changes at fixed intervals (e.g. every 6 months)
	Information systems require multi-factor authentication
	Passwords are stored in a way that makes them unintelligible while they are in force
	Supplier will ensure that deactivated or expired [ ]
	Supplier maintains and updates a record of personnel and subcontractors authorized to access company systems that contain personal data
	Supplier maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed
	Supplier deactivates authentication credentials that have not been used for six months
	Where authentication mechanisms are based on passwords, the password is required to be at least eight characters long

Measures taken to restrict access to its data-processing systems. (cont'd)	State-of-the art encryption applied to all data – whether 'in transit' or 'at rest'
	Regular audits of security procedures
	Employees and other Supplier personnel are trained regarding access to information systems
USE CONTROLS	
Measures used to restrict individuals from accessing personal data to which they do not have access privileges.	Maintain security privilege record/log of individuals having access to personal data
	Access to personal data is restricted to only those individuals who require such access to perform their job function
	Log access and use of information systems containing personal data, registering the access ID, time, authorization granted or denied, and relevant activity.
	Security personnel verify logs to identify any irregularities in access or use and propose remediation efforts for such irregularities, if any, on a monthly basis
	Personnel and subcontractors with access to personal data are subject to confidentiality obligations
	Supplier has controls to avoid individuals assuming access rights they have not been assigned to gain access to personal data they are not authorized to access.
	Supplier has firewalls, anti-virus and anti-malware controls to help avoid malicious software gaining unauthorized access to personal data, in particular malicious software originating from public networks
DISTRIBUTION CONTROLS	
Measures used that are designed to prevent unauthorized reading, copying, changing or removing of personal data during transmission or storage on media.	Personal data that is transmitted over public networks are encrypted
	Supplier tracks disclosures of personal data, including what data has been disclosed, to whom, and at what time
	Supplier imposes restrictions on printing personal data and have procedures for disposing of printed materials that contain personal data
INPUT CONTROLS	
Monitoring and logging measures used to audit inputs, changes, and deletions from its data-processing systems.	Supplier logs the use of its data-processing systems containing personal data
	Logs include ID, time, authorization granted or denied, and relevant activity
	Security personnel verify logs to identify any irregularities in access or use and propose remediation efforts for such irregularities every six months

PURPOSE CONTROLS	
Measures used to limit processing it performs as a data processor to only processing in accordance with the instructions of the data controller.	Supplier restrict internal testing/proofs of concept with live personal data
	When internal testing/proofs of concept uses live personal data for testing, parties provides and documents, the relevant level of security for the processing
	Supplier back up any actual personal data prior to using it for testing
	Supplier use security logs only for their intended security purpose
	When parties are engaged to process special categories of data, parties maintain logical separation between this and other data
	Technical support personnel and subcontractors only have access to personal data when needed
AVAILABILITY CONTROLS	
Measures used to protect against incidental destruction or loss of personal data.	Where party acts as a data processor or subprocessor, party will not initiate any data recovery procedures without the written authorization of NetApp.
	Redundant storage and procedures for recovering personal data are designed to attempt to reconstruct personal data in its original state from before the time it was lost or destroyed
	Supplier uses a variety of industry standard systems to protect against loss of personal data due to power supply failure or line interference
	Supplier backs up copies of personal data at least once a week, unless no personal data has been updated during that period
	Where party acts as a data processor or subprocessor, it stores backup copies of personal data and recovery procedures in a different place from where the primary computer equipment processing the personal data is located.
	Supplier has specific procedures in place governing access to backup copies.
	Supplier logs personal data restoration efforts, including the person(s) responsible, the description of the restored personal data and which data (if any) had to be input manually in the recovery process
	Supplier reviews recovery and backup procedures at least every six months
	Supplier maintains procedures designed to allow for recovery of personal data within seven days
ADMINISTRATIVE CONTROLS	
Measures used to document and track administrative oversight.	Supplier maintains security documents describing its security measures and sets out the relevant procedures and responsibilities of company personnel and subcontractors who have access to personal data

	Supplier maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering personal data
	Supplier has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures
	Supplier will perform a risk assessment before processing any personal data or launching Services
	Supplier retains its security documents for at least five years after they are no longer in effect
TRAINING REQUIREMENTS	
Training requirements of personnel and subcontractors.	Supplier informs their personnel and subcontractors about relevant security procedures and their respective roles
	Supplier also informs their personnel and subcontractors of possible consequences of breaching the security rules and procedures

ANNEX 3

LIST OF SUBPROCESSORS

The controller has given general authorization for Supplier to use the subprocessors contained within Supplier's list located at: [INSERT site address or description of where the master list will be maintained]. A copy of the list current as of the date of execution of this ADDENDUM is attached hereto as Schedule 1 to this Annex 3.

Schedule 1 to Annex 3: Current List of Subprocessors