NetApp

# NETAPP DATA PROCESSING ADDENDUM

This NetApp Data Processing Addendum including its Appendices ("**Addendum**") supplements the Agreement between NetApp, Inc. and/or its affiliates, including the NetApp affiliate performing the Services ("**NetApp**"), and Customer (together the "**Parties**"). To the extent there is a conflict between the Agreement and the terms of this Addendum, the terms of this Addendum will prevail unless otherwise expressly set forth herein.

**1. DEFINITIONS.** Capitalized terms used but not defined in this Addendum have the meanings set forth in the Agreement. In this Addendum:

**1.1.** "**Agreement(s)**" means the applicable written agreement(s) between NetApp and Customer under which NetApp provides Products and/or Services to Customer.

**1.2.** "**Customer Personal Information**" means Personal Information provided by or on Customer's behalf that NetApp Processes as a Data Processor and/or Sub-processor on behalf of Customer in performing the Services.

**1.3.** "**Data Controller**" means an entity which, alone or jointly with others, determines the purposes and means of Processing of Personal Information.

**1.4.** "**Data Processor**" means an entity which Processes Personal Information on behalf of a Data Controller.

**1.5.** "**Data Protection Laws**" mean any applicable laws, regulations, and other legal requirements relating to (a) privacy or protection of Personal Information and / or (b) the Processing of Personal Information, including but not limited to the EU General Data Protection Regulation ("**GDPR**") and the EU Member State data protection laws implementing or supplementing GDPR, the UK General Data Protection Regulation ("**UK GDPR**"), the Swiss Federal Act on Data Protection ("**FADP**"), the Personal Information Protection Law of China ("**PIPL**") and US State Privacy Laws.

**1.6.** "**Data Subject**" has the meaning given to the term under Article 4 of the GDPR.

**1.7.** "**EEA**" means European Economic Area.

**1.8.** "**Effective Date**" means the date of Customer's underlying purchase of NetApp Products or Services involving the Processing of Customer Personal Information.

**1.9.** "**Personal Information**" means (a) any information relating to an identified or identifiable natural person; or (b) is defined as "personal data" or "personal information" by applicable laws or regulations relating to the Processing of information about an identified or identifiable person.

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

**1.11.** "**Products**" means the products provided by NetApp as set forth in the Agreement.

**1.12.** "**Security Incident**" has the meaning assigned to it in Section 8 (Security Incident).

**1.13.** "**Services**" means the services provided by NetApp as set forth in the Agreement. Services may include NetApp's software ("**Software**"), NetApp's as-a-service offerings which are purchased as a subscription for a defined term (as applicable, "**Cloud Services**" or "**StaaS Services**" ), NetApp's consulting services ("**Professional Services**") and/or NetApp's generally available technical support and maintenance services programs ("**Support Services**") which may be further specified in service descriptions or statements of work.

**1.14.** "**SCCs**" mean (i) the standard contractual clauses (2021/914) published by the European Commission including any updated, amended or successor clauses, as set out at Appendix 1 ("**Approved EEA SCCs**"); and (ii) the UK Addendum to the Approved EEA SCCs, as set out at Appendix 1 ("**UK Addendum**").

**1.15.** "**Sub-processor**" means an entity which Processes Personal Information on behalf of a Data Processor.

**1.16.** "**Third Country**" means any country for which as the context may require, the European Commission or the relevant UK Secretary of State has not confirmed a suitable level of data protection on the basis of an adequacy decision.

**1.17.** "**UK**" means the United Kingdom.

**1.18.** "**US State Privacy Laws**" means all applicable US state privacy laws and their implementing regulations, as amended or superseded from time to time, including but not limited to the California Consumer Privacy Act of 2018 (as amended), (the "**CCPA**") including as modified by the California Privacy Rights Act of 2020 ("**CPRA**"), as applicable to Customer Personal Information. The terms, "Contractor", "Service Provider", "Share", "Shared" "Sharing", "Sale", "Selling" and "Third Party" shall have the meaning defined in the US State Privacy Laws. In the event of any conflict of means of the defined terms in the US State Privacy Laws, the meaning from the law applicable to the state of residence of the relevant consumer applies.

**2. APPLICABILITY; ROLES OF PARTIES.** This Addendum applies to the extent that NetApp Processes Customer Personal Information as a Data Processor and/or Sub-processor on behalf of Customer in performing Services. As between the parties, NetApp acts as a Data Processor and/or Sub-processor and Customer acts as a Data Controller and/or Data Processor of the Customer Personal Information when this Addendum applies. Where Customer is not the Data Controller, upon request, Customer will confirm the identity and contact details of the Data Controller to NetApp. To the extent that NetApp acts as a Data Processor/Sub-processor, NetApp will Process Customer Personal Information solely to provide Services in accordance with the Agreement or other documented instructions that Customer may provide (whether in written or electronic form) in accordance with the Agreement, or as otherwise required by applicable law (including with regard to transfers of Customer Personal Information to a Third Country), which collectively will comprise Customer's complete instructions to NetApp regarding the Processing of Customer Personal Information. If NetApp is required by applicable law to Process Customer Personal Information other than in accordance with the Agreement or other documented

instructions of Customer, NetApp will inform Customer of that legal requirement prior to such Processing, unless prohibited by applicable law. When acting as a Data Processor/Sub-processor, NetApp shall not, without the prior written consent of Customer (which Customer shall not unreasonably withhold) in each instance: **(i)** Sell or Share Customer Personal Information, **(ii)** retain, use, or disclose Customer Personal Information for any purpose other than the Services, those purposes set forth in this Addendum, and as otherwise permitted by Data Protection Laws; **(iii)** retain, use, or disclose Customer Personal Information outside of the direct business relationship between the parties, and **(iv)** except as is necessary to fulfill its obligations to perform the Services as permitted under Data Protection Laws and this Addendum, combine Customer Personal Information with Personal Information obtained from, or on behalf of, sources other than Customer. NetApp will reasonably cooperate with Customer's reasonable and appropriate steps to confirm NetApp's use of Customer Personal Information is consistent with Customer's obligations under Data Protection Laws. Customer may, upon reasonable advanced notice to NetApp, take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Information. NetApp will notify Customer if NetApp determines it can no longer meet its obligations under the CPRA or other Data Protection Laws requiring the same notification.

**3. CONFIDENTIALITY.** NetApp will require NetApp personnel who will be provided access to, or will otherwise Process, Customer Personal Information, to be under an appropriate obligation of confidentiality and protect Customer Personal Information consistent with the standards set forth in this Addendum.

**4. COMPLIANCE WITH LAWS**.

**4.1.** NetApp will comply with all Data Protection Laws applicable to NetApp as a Data Processor/Sub-processor Processing Customer Personal Information on Customer's behalf, to the extent NetApp engages in such Processing.

**4.2.** Customer will comply with all Data Protection Laws applicable to Customer with respect to such Processing of Customer Personal Information.

**4.3.** Customer will also:

**(i)** be responsible for ensuring that all Customer Personal Information is adequate, relevant and not excessive in relation to the purposes for which Customer Personal Information is Processed by NetApp;

**(ii)** remain responsible for the quality and accuracy of the Customer Personal Information disclosed to NetApp;

**(iii)** ensure the Customer takes all necessary precautions to ensure the security of any Customer Personal Information, during transit to NetApp; and

**(iv)** ensure it complies with its obligation to provide sufficient information to Data Subjects with regards to the Processing of their Personal Information by NetApp on behalf of the Customer.

**5. SUB-PROCESSORS.** Customer agrees that NetApp has Customer's general authorization to use Sub-processors (including NetApp affiliates) to Process Customer Personal Information for purposes of providing the Services to Customer, provided that NetApp will impose on its Sub-processors data protection obligations that are at least as protective of Customer Personal Information as those set forth in this Addendum. NetApp will make a list of Sub-processors available to Customer by posting it to a Customer-accessible site (the Agreed List). NetApp will notify Customer of any new Sub-processor by posting an updated list of Sub-processors on the Agreed List at least thirty (30) days before authorizing any new Sub-processor to Process Customer Personal Information. Customer may object to such addition by written notice to NetApp by way of email to dataprotection@netapp.com. NetApp will be liable for the acts or omissions of its Sub-processors to the same extent as if the acts or omissions were performed by NetApp. NetApp will disclose Customer Personal Information only to Sub-processors or as otherwise expressly authorized under the Agreement (including this Addendum) or as required by law.

**6. DATA TRANSFERS.** In providing the Services, NetApp and its Sub-processors may transfer and access Customer Personal Information to and from other countries (including Third Countries) where they have operations, or as otherwise required by applicable law. NetApp will implement appropriate measures to protect Customer Personal Information in accordance with this Addendum regardless of the jurisdiction in which it or the recipient is located, including by complying with Chapter V of the GDPR and the UK GDPR as applicable and necessary.

**7. SECURITY.** NetApp will implement appropriate technical and organizational safeguards designed to protect Customer Personal Information in its possession or control against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to such data in accordance with Annex **II** of Appendix 2. NetApp may modify such safeguards from time to time, provided that such modifications will not materially reduce the overall level of protection for Customer Personal Information.

**8. SECURITY INCIDENT**. If NetApp becomes aware that a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Customer Personal Information in the possession or control of NetApp (a "**Security Incident**") has occurred, NetApp will notify Customer promptly and without undue delay, in accordance with legal obligations and unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Such notification will, to the extent possible, include information about the nature and likely consequences of the Security Incident and how to request additional information if required.

**9. AUDIT AND INSPECTIONS**. NetApp shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer. Notwithstanding anything to the contrary in the Agreement, and taking into account the nature of the Processing and the Services being provided, the

following processes will be used to satisfy any audit or inspection requests by or on behalf of Customer and to demonstrate compliance with applicable obligations of NetApp as set forth in this Addendum and under Article 28 of the GDPR/UK GDPR:

**9.1. Cloud Services.** For applicable Cloud Services, at least once per calendar year, NetApp will obtain an ISO/IEC 27001:2013 certification or retain an independent third-party auditor to prepare a Services Organization Control 2 (Type II) report or industry-standard successor report ("**Report**"). Upon Customer's written request, NetApp will provide to Customer within a reasonable time at no cost a copy of the most recent Report, up to once per year.

**9.2. Professional Services and Support Services**. For Professional Services and Support Services, NetApp will, upon Customer's written request, up to once per year **(i)** provide to Customer at no cost a copy of the most recent third-party certification or Report for such Services, if NetApp has obtained a certification or Report for such Services; or **(ii)** provide Customer with reasonable information concerning its data protection measures for such Services to help Customer comply with its audit obligations or a competent supervisory authority's request ("**Supplemental Information**").

**9.3. Reports and Supplemental Information.** Such Reports and Supplemental Information will be NetApp's Confidential Information under the confidentiality provisions of the Agreement.

**9.4. Customer Access.** If the Reports and Supplemental Information, following review by Customer, are deemed (in Customer's reasonable and good faith opinion) not to be sufficient to demonstrate compliance with the obligations laid down in this Addendum, then NetApp will permit Customer (including its mandated auditors) access and inspection in terms of an onsite audit, only insofar as required by law.

**9.5. Regulator Access.** NetApp will permit applicable regulator access and inspection as required by law and when on-site documentary and evidence review by the regulator is deemed insufficient by the regulator for their purpose of regulating the Customer or NetApp**.**

**10. REQUESTS OR COMPLAINTS FROM DATA SUBJECTS**. NetApp will promptly notify Customer, unless prohibited by applicable law, if NetApp receives: **(i)** any privacy related requests from a Data Subject with respect to Customer Personal Information Processed by NetApp in its role as Customer's Data Processor/Sub-processor, including but not limited to opt-out requests, requests for access and/or rectification, blocking, erasure, requests for data portability, and all similar requests; or **(ii)** any complaint relating to the Processing by NetApp of Customer Personal Information, including allegations that such Processing infringes on a Data Subject's rights. Customer is responsible for responding to such requests and complaints from Data Subjects. Taking into account the nature of the Processing, NetApp will assist the Customer by appropriate technical and organizational measures, insofar as reasonably possible, for the fulfillment of the Customer's obligation to respond to such requests or complaints.

**11. DURATION; RETURN OR DISPOSAL**. This Addendum is effective as of the Effective Date. The duration of the Processing will be the term of the Agreement or until all Customer Personal Information has been returned or deleted in accordance with the following. Upon termination or expiration of the Agreement for any reason, **(i)** for Cloud Services, Customer will be entitled to retrieve its Customer Personal Information in accordance with the Agreement, and NetApp will delete Customer Personal Information from the Services following such retrieval period unless otherwise required by applicable law; or **(ii)** for StaaS Services, Professional Services or Support Services, NetApp will delete or return Customer Personal Information in its possession or control in accordance with the Agreement, unless otherwise required by applicable law.

**12. ADDITIONAL PROVISIONS FOR THE EEA + UK + SWITZERLAND.** The following additional provisions apply with respect to the Processing of Customer Personal Information of Data Subjects of the EEA, UK and Switzerland:

**12.1.** Taking into account the nature of the Processing and the information available to NetApp, NetApp will make reasonable efforts to assist Customer upon request in fulfilling any obligations Customer may have under GDPR, UK GDPR or Swiss law to: **(a)** provide notification of a Security Incident to the supervisory authorities or affected Data Subjects, **(b)** perform a data protection impact assessment (and/or consult with a supervisory authority in respect of such an assessment), to the extent required under Data Protection Laws. NetApp shall immediately inform Customer, if in NetApp's opinion, instructions given by the Customer in relation to Customer Personal Information of data subjects of the EEA, UK or Switzerland infringe applicable data protection provisions.

**12.2.** To the extent that Customer transfers Customer Personal Information to NetApp in a Third Country and such Customer Personal Information concerns: **(1)** EEA and/or Swiss data subjects, the EEA/Swiss Addendum at Appendix 1 will apply; and **(2)** UK data subjects, the UK Addendum at Appendix 1 will apply.

**12.3.** Nothing in this Addendum modifies or amends the terms of the SCCs. To the extent there is a conflict between the SCCs and the terms of this Addendum, the SCCs will prevail.

## APPENDIX 1: EEA / UK / SWISS ADDENDUM

**INCORPORATION AND INTEGRATION OF THE APPROVED EEA SCCs**

1. As used herein the "**Approved EEA SCCs**" mean the Standard Contractual Clauses (2021/914) published by the European Commission on the 4th of June 2021 including any updated, amended or successor clauses.

2. The terms of the Approved EEA SCCs are deemed incorporated into this EEA/UK/Swiss Addendum by reference, including the Annexes to the Approved EEA SCCs set out in Appendix 2, with the following specifications:

   **a.** To the extent that Customer is a Data Controller of the transferred Personal Information, Module 2 (controller to processor) of the Approved EEA SCCs will govern such transfers.
   **b.** To the extent that Customer is a Data Processor of the transferred Personal Information, Module 3 (processor to processor) of the Approved EEA SCCs will govern such transfers.
   **c.** Clause 7 (Docking clause) of the Approved EEA SCCs shall apply.
   **d.** For the purposes of Clause 9(a) (Use of sub-processors) of the Approved EEA SCCs, option 2 (General Written Authorization) applies and the relevant time period is 30 days. Subject to and in accordance with Clause 9(a) in Module 2 and Module 3 (if applicable), NetApp has Customer's general authorization to engage the Sub-processors from the following Agreed List. To the extent that "NetApp" for the purposes of the Agreement does not also include affiliates, the NetApp Affiliates are also Sub-processors.
   **e.** The independent dispute resolution optional language in Clause 11 (Redress) of the Approved EEA SCCs does not apply.
   **f.** For the purposes of Clause 17 (Governing law) of the Approved EEA SCCs, option 1 applies and the law of Ireland shall apply.
   **g.** For the purposes of Clause 18 (Choice of forum and jurisdiction) of the Approved EEA SCCs, the courts of Ireland shall resolve any dispute arising from the Approved EEA SCCs.

3. **Switzerland: Specific amendments to the Approved EEA SCCs in relation to Customer Personal Information of Swiss Data Subjects**

   **a.** It is agreed that if a transfer of Customer Personal Information is made from Switzerland, the Approved EEA SCCs shall be deemed to be amended as follows to apply to that transfer (and without limiting or affecting the application of the Approved EEA SCCs otherwise):

      **i.** General and specific references in the Approved EEA SCCs to Regulation (EU) 2016/679 or "that Regulation" or EU or Member State law have the same meaning as the equivalent reference in data protection laws and regulations of Switzerland including the Swiss Federal Act on Data Protection ("**FADP**");
      **ii.** The "competent supervisory authority" is the Federal Data Protection and Information Commissioner ("**FDPIC**") for the purposes of Clause 13 (Supervision) of the Approved EEA SCCs;
      **iii.** The term "Member State" will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of exercising their rights under privacy laws in their place of habitual residence (Switzerland) in accordance with Clause 18(c) (Choice of forum and jurisdiction) of the Approved EEA SCCs;
      **iv.** The term "personal data" shall be deemed to include the data relating to an identified or identifiable legal entity to the extent such data is protected under the FADP; and
      **v.** Any amendments required from time to time by the FDPIC in order to comply with the FADP.

4. **United Kingdom: International Data Transfer Addendum to the Approved EEA SCCs**

   **a.** This section 4(a) of Appendix 1 (the "**UK Addendum**") incorporates the Mandatory Clauses of Part 2: Mandatory Clauses of the UK Addendum, being the template International Data Transfer Addendum to the EU Commission Standard Contractual Clauses B.1.0 issued by the UK Information Commissioner's Officer ("**ICO**") and laid before UK Parliament in accordance with s119A of the UK Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
   **b.** Any reference to the "**Addendum EU SCCs**" in the Mandatory Clauses shall be a reference to the Approved EEA SCCs, including the Appendix Information (set out at Appendix 2), and with only the Modules, clauses or optional provisions of the Approved EEA SCCs brought into effect as set out in the EEA/Swiss Addendum at Appendix 1 (without regard to the specific amendments made for Customer Personal Information of Swiss Data Subjects) and as amended in accordance with the UK Addendum.
   **c.** Either Party may end this UK Addendum under Clause 19 of the UK Addendum.

## APPENDIX 2: ANNEXES TO THE SCCS

**ANNEX 1**

- **MODULE 2: Transfer controller to processor**: if Customer is a Data Controller of Customer Personal Information, then Module 2 SCCs applies.
- **MODULE 3: Transfer processor to processor**: if Customer is a Data Processor of Customer Personal Information, then Module 3 SCCs applies.

### A. LIST OF PARTIES

| **Data exporter(s):** *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union or the UK* | |
|---|---|
| Company Legal Name:<br>*(Please specify the data exporter's legal name)* | *The Customer who entered into the Agreement with NetApp* |
| *Official registration number, company number or similar identifier (if any):* | *As specified in the Agreement* |
| Address:<br>*(Please insert the data exporter's business address)* | *As specified in the Agreement* |
| Contact person's name, position and contact details:<br>*(Please complete for the data protection and privacy responsible person in your company)* | *The Customer shall designate to NetApp a single point of contact (and/or Data Protection Officer) for all matters related to the Addendum and the Processing of Customer Personal Information* |
| Signature and Date of Signature: | *As appears in the Agreement's signature block* |
| Activities relevant to the data transferred under these SCCs: | *As described in the Agreement or relevant service agreement(s)* |
| Role (controller/processor): | *Where applicable, either:*<br>▪ *a Data Controller (where determining the purpose and means of processing); or*<br>▪ *a Data Processor (where acting on behalf of its own end-customer).* |

| **Data importer(s):** *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection* | |
|---|---|
| *Company Legal Name:* | *NetApp, Inc.* |
| *Official registration number, company number or similar identifier:* | *77-0307520* |
| *Address:* | *3060 Olsen Drive*<br>*San Jose, CA 95128*<br>*United States* |
| *Contact person's name, position and contact details:* | *dataprotection@netapp.com*<br>*Phone: +1 404-822-6000* |
| *Signature and Date of Signature:* | *As appears in the Agreement's signature block* |
| *Activities relevant to the data transferred under these SCCs:* | *As described in the Agreement or relevant service agreement(s)* |
| *Role (controller/processor):* | *Data Processor and/or Sub-processor* |

## B. DESCRIPTION OF PROCESSING / TRANSFER

***Categories of data subjects whose personal information is transferred***

Unless otherwise specified by the Customer, Customer Personal Information relates to the following categories of Data Subjects:

- Employees, contractors and temporary workers (current, former, prospective) of Customer;
- NetApp's Customers' collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., Customers, clients, patients, visitors, etc.) and other Data Subjects that are users of NetApp's or its Customers' services; and
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of NetApp's Customer and/or use communication tools such as apps and websites provided by NetApp or its Customers.

***Categories of personal information transferred***

Customer Personal Information that may be collected and/or Processed includes data in multiple formats, including email, documents and other electronic forms. Depending on the applicable use of the Services, NetApp may collect and/or Process the following categories of Personal Information:

- **Customer Information**: this includes information like an end-user's company name, job title, account number, Customer identifier, or other Information that relates to an end-user as a Customer of NetApp.
- **Commercial Information**: this includes payment related data, financial or account information, records of Products or Services purchased, obtained or considered, or other purchasing or consuming histories or tendencies of the Customer, and other information necessary to collect and process payment for Products and Services ordered by Customer.
- **Individual Identifiers**: this includes information like an end-user's name, email address, physical address, telephone number, login alias, IP address or other Information that identifies the end-user regardless of their relationship to NetApp.
- **Electronic Network Information**: this includes information like usage data, functional data, AutoSupport data, device data, browser information, and internet or network activity information, such as activity on our websites and services, data collected through cookies, pixel tags and other similar technologies, and other information that is generated through the end-user's use of our websites, Products and/or Services.
- **Personal Information contained with Customer Content**: this includes any personal information that may be shared by Customer with NetApp in order for us to provide certain NetApp Services.

***Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).***

The transfer of Customer Personal Information may occur on a continuous or one-off basis depending on the Products or Services outlined in the underlying Agreement(s).

***Nature of the processing***

Where NetApp is the Data Processor/Sub-processor, Processing may include the collection, use, analysis, storage, and deletion, including the sharing of data with authorized Sub-processors for the purposes of providing, monitoring, and improving products or services.

Customer Personal Information may be subject to the following basic Processing activities:

- use of Personal Information to set up, operate, monitor and provide Products or Services (including operational and technical support), including communication to Authorized Users;
- provision of Professional Services;
- release, development and upload of any fixes or upgrades to the Products or Services;
- storage, back up and restoration of Personal Information stored in the Products or Services;
- computer processing of Personal Information, including data transmission, data retrieval, and data access;
- network access to allow Personal Information transfer;
- continuous improvement of Product or Service features and functionalities provided as part of the Services; monitoring, troubleshooting and administering the underlying service infrastructure and database; and
- security monitoring, network-based intrusion detection support, and penetration testing.

***Purpose(s) of the data transfer and further processing***

Where NetApp is the Data Processor/Sub-processor, the data transfer is required to provide the Products and Services, ancillary support and Support Services, and monitor, develop and improve Products and Services.

***Data Retention Period***

NetApp will retain Personal Information for as long as needed or permitted in light of the purpose(s) for which it was obtained per the underlying Agreement and consistent with applicable law.

Transfers to Sub-processors shall be on the same basis.

## C. COMPETENT SUPERVISORY AUTHORITY

In respect of Modules 2 and 3 of the Approved EEA SCCs (as applicable), the supervisory authority is determined in accordance with Clause 13(A) of the Approved EEA SCCs and shall be the Irish Data Protection Commission.

For Switzerland: the “competent supervisory authority” is the FDPIC.

## ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES ("TOMs")

The TOMs in this Annex II are without prejudice to any more stringent and/or additional TOMs that may be agreed upon and/or any other relevant contractual arrangement between the parties.

### TECHNICAL AND ORGANISATIONAL MEASURES

NetApp takes reasonable and appropriate measures to secure the Personal Information processed in connection with this Data Processing Addendum, taking into account the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of Processing and the risks involved in the Processing for the Data Subject. NetApp further makes available to its customers certain features and functionalities of NetApp Products and Services, such as support for encryption or pseudonymization, including during transmission of Personal Information, to help customers implement reasonable and appropriate measures to secure the Personal Information. For those Products and Services that are covered under the scope of this Data Processing Addendum, NetApp implements at least the security controls , as described in the NetApp Information Security Addendum, available at https://www.netapp.com/pdf.html?item=/media/115701-netapp-info-security-addendum.pdf, together with the additional terms set forth below. NetApp carries out regular checks to ensure that these security measures continue to be in place and are functioning as designed

### 1. ORGANIZATIONAL CONTROLS

**1.1** **Organizational Measures.** NetApp maintains policies, procedures, and protocols designed to limit the collection, use, and sharing of Personal Information to authorized individuals and entities, including (a) security policies in place for end-users and administrators of corporate systems; (b) Global Privacy Policy; (c) Global Data Governance Policy; (d) Global Retention Schedule; (e) Global Procurement Process to ensure vendor/supplier security standards and controls; (f) Privacy by Design validation program; (g) contracting protocols to pass privacy obligations to Data Processors and Sub-processors; and (h) regular reviews of Business Continuity, Disaster Recovery plans, and security incident response.

### 2. DELETION AND DISPOSAL CONTROLS

**2.1** **Data Retention and Deletion.** NetApp maintains a data governance policy and related controls designed to ensure that Personal Information is not retained in records for longer than required under the lawful basis for Processing, including (a) the de-identification of records containing Personal Information once the Personal Information is no longer necessary for the purpose of record keeping; (b) protocols for the sanitization and/or disposal of NetApp owned equipment and media containing Personal Information; and (c) protocols for the sanitization of customer equipment and media under return authorization.