DATA PROCESSING ADDENDUM

Dated July 19, 2024

This Data Processing Addendum ("**DPA**") supplements the Agreement entered into between the Customer and Qumulo (the "**Parties**") in relation to the Processing of Covered Data (each as defined below).

1. DEFINITIONS

1.1 Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. The following capitalized terms used in this DPA will be defined as follows:

"**Administration Data**" means:

(a) contact details relating to, and the content of correspondence with Customer's main account holder or administrator; and

(b) support enquiries submitted by or on behalf of Customer or its Authorized Users.

"**Adequacy Decision**" means:

(a) in respect of transfers of Personal Data relating to Data Subjects in the EEA, a decision by the European Commission under Article 45 of the EU GDPR (including, without limitation, Commission Implementing Decision C(2023) 4745 on the adequate level of protection of personal data under the EU-US Data Privacy Framework);

(b) in respect of transfers of Personal Data relating to Data Subjects in the UK, Part 3 of Schedule 21 to the UK Data Protection Act 2018 and regulations made by the UK Secretary of State under section 17A of the UK Data Protection Act 2018 (including, without limitation, the Data Protection (Adequacy) (United States of America) Regulations 2023); and

(c) in respect of transfers of Personal Data relating to Data Subjects in a jurisdiction where Applicable Data Protection Laws prohibit the transfer of Personal Data to a recipient in another jurisdiction in the absence of adequate safeguards in respect of the Processing of that Personal Data by the recipient, a decision or designation equivalent to (a) and (b) above by the relevant national authority, regulatory body or statutory instrument under Applicable Data Protection Laws in that jurisdiction.

"**Agreement**" means the agreement between Customer and Qumulo incorporating the following terms:

(a) in respect of the Customer's use of the Products, the End User Agreement as found at https://qumulo.com/terms-hub/agreements/ ("**EULA**"); and

(b) in respect of the Customer's receipt of the Subscription Services, the SaaS Subscription Terms and Conditions as found at https://qumulo.com/terms-hub/agreements/ ("**SaaS Terms**").

(c) in respect of the Customer's use of the Cloud Native Qumulo Software, the Cloud Native Qumulo Offering Subscription Terms and Conditions as found at https://qumulo.com/terms-hub/agreements/ ("**CNQ Terms**")

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time.

"**Controller Purposes**" means: (a) undertaking internal research and development to test, improve and alter the functionality of the Subscription Services, the Products and any of Qumulo's other products and services; (b)(creating anonymized and aggregated datasets for training or evaluation of the Subscription Services, the Products and any of Qumulo's other products and services; and (c) administering Qumulo's relationship with Customer under the Agreement.

"**Covered Data**" means Personal Data that is: (a) provided by or on behalf of Customer to Qumulo in connection with the Services; or (b) obtained, developed, produced or otherwise Processed by Qumulo, or its agents or subcontractors, for purposes of providing the Services, in each case as further described in Schedule 1.

"**Data Subject**" means a natural person whose Personal Data is Processed.

"**Deidentified Data**" means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"**EEA**" means the European Economic Area including the European Union ("**EU**").

"**Effective Date**" means the later of: (a) the date the Customer enters into the Agreement; and (b) the date first listed above.

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as defined in section 3 of the UK Data Protection Act 2018 or, where applicable, the equivalent provision under Swiss data protection law.

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein.

"**Personal Data**" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Security Incident**" means an actual or reasonably suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

"**Services**" means the services to be provided by Qumulo pursuant to the Agreement, being (as applicable) the Subscription Services to be provided under the SaaS Terms and/or Support provided under the EULA.

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"**Sub-processor**" means an entity appointed by Qumulo to Process Covered Data on its behalf.

"**Swiss Data Protection Laws**" means the Swiss Federal Act on Data Protection of 25 September 2020 ("**FADP**") and the Swiss Data Protection Ordinance of 31 August 2022, and any new or revised version of these laws that may enter into force from time to time.

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

"**US Data Protection Laws**" means, to the extent applicable, federal and state laws relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States.

"**Usage Data**" means any Personal Data contained in the Platform Data and Statistical Data (as applicable).

2. INTERACTION WITH THE AGREEMENT

2.1 As of the Effective Date, this DPA is incorporated into and forms an integral part of the Agreement. This DPA supplements and (in case of contradictions) supersedes the Agreement and any other terms agreed between the Parties with respect to any Processing of Covered Data.

3. ROLE OF THE PARTIES

The Parties acknowledge and agree that:

(a) save as set out in clause 3(c), for the purposes of the GDPR, Qumulo acts as "processor" or "sub-processor" (as each term defined in the GDPR) in the performance of its obligations under the Agreement and this DPA. Qumulo's function as processor or sub-processor will be determined by the function of the Customer:

(i) where Customer acts as a "controller" (as defined in the GDPR), Qumulo acts as a processor;

(ii) where Customer acts as a processor on behalf of another controller, Qumulo acts as a sub-processor;

(b) for the purposes of the US Data Protection Laws, Qumulo will act as a "service provider" or "processor" (each as defined in US Data Protection Laws), as applicable, in its performance of its obligations under the Agreement and this DPA; and

(c) for the purposes of the GDPR, Qumulo acts as a controller with respect to its Processing of the Usage Data and Administration Data for the Controller Purposes.

4. DETAILS OF DATA PROCESSING

4.1 The details of the Processing of Personal Data under the Agreement and this DPA (such as subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in **Schedule 1** to this DPA.

4.2 Other than in respect of its Processing of Usage Data and Administration Data for the Controller Purposes, Qumulo will only Process Covered Data on behalf of and under the instructions of Customer and in accordance with Applicable Data Protection Laws. The Agreement and this DPA shall constitute Customer's instructions for the Processing of Covered Data. Customer may issue further written instructions in accordance with this DPA. Without limiting the foregoing, Qumulo is prohibited from:

(a) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration;

(b) sharing Covered Data with any third party for cross-context behavioral advertising;

(c) retaining, using, or disclosing Covered Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Applicable Data Protection Laws;

(d) retaining, using, or disclosing Covered Data outside of the direct business relationship between the Parties; and

(e) except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that Qumulo receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

4.3 Upon Customer's reasonable request, Qumulo will provide Customer with information reasonably necessary to demonstrate Qumulo's compliance with its obligations as set forth in this DPA and to enable Customer to conduct and document any data protection assessments required under Applicable Data Protection Laws. In addition, Qumulo will notify Customer promptly if Qumulo determines that it can no longer meet its obligations under Applicable Data Protection Laws.

4.4 Qumulo will promptly inform Customer if, in its opinion, an instruction from Customer or Customer's controller infringes Applicable Data Protection Laws.

5. CONFIDENTIALITY AND DISCLOSURE

5.1 Qumulo shall:

(a) limit access to Covered Data to personnel who have a business need to have access to such Covered Data; and

(b) will ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement, including duties of confidentiality with respect to any Covered Data to which they have access.

6. SUB-PROCESSORS

6.1 Qumulo may Process Covered Data anywhere that Qumulo or its Sub-processors maintain facilities, subject to the remainder of this clause 6.

6.2 Customer grants Qumulo the general authorisation to engage the Sub-processors listed at https://trust.qumulo.com/subprocessors, subject to clause 6.3.

6.3 Qumulo will enter into a written agreement with each Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than Qumulo's obligations under this DPA.

6.4 Qumulo will provide Customer with at least fifteen (15) days' notice of any proposed changes to the Sub-processors it uses to Process Covered Data. Customer may object to Qumulo's use of a new Sub-processor (including, where applicable, when exercising its right to object under clause 9(a) of the SCCs) by providing Qumulo with written notice of the objection within ten (10) days after Qumulo has provided notice to Customer of such proposed change (an "**Objection**"). If Customer does not object to the engagement within the Objection period, consent regarding the engagement will be assumed. In the event

Customer objects to Qumulo's use of a new Sub-processor, Customer and Qumulo will work together in good faith to find a mutually acceptable resolution to address such Objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, which shall not exceed thirty (30) days, either Party may, as its sole and exclusive remedy, terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to the other Party. During any such Objection period, Qumulo may suspend the affected portion of the Services.

7. DATA SUBJECT RIGHTS REQUESTS

7.1 Other than in respect of Qumulo's Processing of Usage Data and Administration Data for the Controller Purposes, as between the Parties, Customer will have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Covered Data under Applicable Data Protection Laws (each, a "**Data Subject Request**").

7.2 Qumulo will promptly forward to Customer without undue delay any Data Subject Request received by Qumulo or any Sub-processor and may advise the individual to submit their request directly to Customer.

7.3 Qumulo will provide Customer with reasonable, best effort assistance as necessary for Customer to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests.

8. SECURITY

8.1 Qumulo will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure security of Covered Data, including, without limitation, protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage of or to it. When assessing the appropriate level of security, account will be taken in particular of the nature, scope, context and purpose of the Processing as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data.

8.2 Qumulo will implement and maintain as a minimum standard the measures set out in Schedule 2.

9. INFORMATION AND AUDITS

9.1 Customer will have the right to audit Qumulo's compliance with this DPA. The Parties agree that all such audits will be conducted:

(a) upon reasonable written notice to Qumulo;

(b) only once per year; and

(c) only during Qumulo's normal business hours.

9.2 To conduct such audits, Customer may engage a third-party auditor subject to such auditor complying with the requirements under clause 9.1 and provided that such auditor is suitably qualified and independent.

9.3 To request an audit, Customer must submit a detailed proposed audit plan to Qumulo at least two weeks in advance of the proposed audit date. Qumulo will review the proposed audit plan and work cooperatively with Customer to agree on a final audit plan. All such audits must be conducted subject to the agreed final audit plan and Qumulo's health and safety or other relevant policies.

9.4 Customer will promptly notify Qumulo of any non-compliance discovered during an audit.

9.5 Customer will bear the costs for any audit initiated by Customer, unless the audit reveals material non-compliance with the requirements of this DPA.

9.6 Upon request, Qumulo will provide to Customer documentation reasonably evidencing the implementation of the technical and organizational data security measures in accordance with industry standards. Qumulo may, in its discretion, provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company. If the requested audit scope is addressed in such a certification produced by a qualified third-party auditor within twelve (12) months of Customer's audit request and Qumulo confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report

9.7 Qumulo will audit its Sub-processors on a regular basis and will, upon Customer's request, confirm their compliance with Applicable Data Protection Laws and the Sub-processors' contractual obligations.

9.8 Customer may take reasonable and appropriate steps to: (a) ensure that Qumulo uses Covered Data in a manner consistent with Customer's obligations under Applicable Data Protection Laws; and (b) upon reasonable notice, stop and remediate the unauthorized use of Covered Data.

10. SECURITY INCIDENTS

Qumulo will notify Customer in writing without undue delay after becoming aware of any Security Incident, and reasonably cooperate in any obligation of Customer under Applicable Data Protection Laws to make any notifications, such as to Data Subjects or supervisory authorities. Qumulo will take reasonable steps to contain, investigate, and mitigate any Security Incident, and will send Customer timely information about the Security Incident, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation. Qumulo's notification of or response to a Security Incident under this clause 10 will not be construed as an acknowledgement by Qumulo of any fault or liability with respect to the Security Incident.

Qumulo will provide reasonable assistance with Customer's investigation of the possible Security Incident and any notification obligation of Customer under Applicable Data Protection Laws, such as in relation to individuals or supervisory authorities.

11. DELETION AND RETURN

Qumulo will, within thirty (30) days of the date of termination or expiry of the Agreement (a) if requested to do so by Customer within that period, return a copy of all Covered Data or provide a self-service functionality allowing Customer to do the same; and (b) delete all other copies of Covered Data Processed by Qumulo, other than Administration Data and Usage Data Processed by Qumulo for the Controller Purposes.

12. CONTRACT PERIOD

This DPA will commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Qumulo's deletion of all Covered Data as described in this DPA.

13. STANDARD CONTRACTUAL CLAUSES

13.1 The Standard Contractual Clauses shall, as further set out in Schedule 3, apply to the transfer of any Covered Data from Customer to Qumulo, and form part of this DPA, to the extent that Qumulo is not in a

country, territory or specified sector, or not certified under a scheme, that is subject to an Adequacy Decision and one of the following applies:

(a) the GDPR or Swiss Data Protection Laws applies to the Customer when making that transfer; or

(b) the Applicable Data Protection Laws that apply to the Customer when making that transfer (the "Exporter Data Protection Laws") prohibit the transfer of Covered Data to Qumulo under this DPA in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of that Covered Data, and any one or more of the following applies:

(i) the relevant authority with jurisdiction over the Customer's transfer of Covered Data under this DPA has not formally adopted standard data protection clauses or another transfer mechanism under the Exporter Data Protection Laws; or

(ii) such authority has issued guidance that entering into standard contractual clauses approved by the European Commission would satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(iii) entering into standard contractual clauses approved by the European Commission would otherwise reasonably satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(c) the transfer is an "onward transfer" (as defined in the applicable module of the SCCs).

13.2 The Parties agree that execution of the Agreement shall have the same effect as signing the SCCs.

14. DEIDENTIFIED DATA

If Qumulo receives Deidentified Data from or on behalf of Customer, then Qumulo will:

(a) take reasonable measures to ensure the information cannot be associated with a Data Subject.

(b) publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information.

(c) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

15. GENERAL

15.1 The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

15.2 The Parties agree to negotiate in good faith any amendments to this DPA as may be required in connection with changes in Applicable Data Protection Laws.

15.3 If any court or competent authority decides that any term of this DPA is held to be invalid, unlawful, or unenforceable to any extent, such term will, to that extent only, be severed from the remaining terms, which will continue to be valid to the fullest extent permitted by law.

15.4 This DPA and the Agreement set forth the entire agreement between the Parties with respect to the subject matter hereof.

SCHEDULE 1

DETAILS OF PROCESSING

A. List of Parties

	Controller	**Processor**
Role	Data exporter (controller)	Data importer (processor)
Contact person	The account administrator contact provided by Customer to Qumulo.	Ilana Trager, Director of Security and Privacy Compliance, security@qumulo.com.
Activities relevant to the transfer	The receipt of the Services under the Agreement.	The performance of the Services under the Agreement.

B. Description of Processing

Data transferred by Customer to Qumulo

	Subscription Services (SaaS Terms)
Categories of Data Subjects	Authorized Users. Customer's end users, customers, employees, agents, contractors and others whose data Customer uploads to the Subscription Services ("**Customer Data Subjects**")
Categories of Personal Data	Authorized Users Name, email address, role at Customer. Customer Data Subjects Any Personal Data that Customer or its Authorized Users upload to the Subscription Services.
Special categories of Personal Data	Data relating to a Customer Data Subject's health, to the extent uploaded by Customer to the Subscription Services.
Frequency of the transfer	Continuous
Subject matter and nature of the transfer and Processing	Collection, storage, erasure and rectification in connection with the provision of Subscription Services.
Purposes of the transfer and further Processing	The provision of the Subscription Services, including: ● Granting Authorized Users access to the Subscription Services;

	• Storage and management of Personal Data by Customer through the Subscription Services.
Retention period	For the duration of the Agreement.
Sub-processor(s)	As set out at https://trust.qumulo.com/subprocessors

Data collected by Qumulo in connection with the provision of the Services

	Subscription Services (SaaS Terms)	**Support (EULA)**
Categories of Data Subjects	Authorized Users.	Customer's employees, agents, contractors and others to whom Customer grants access to the Products ("**Product Users**").
Categories of Personal Data	Support requests submitted by the Authorized User, information relating to Authorized User's use of the Subscription Services.	Name, email address, role at Customer, support requests submitted by the Authorized User, Statistical Data relating to the Product User's use of the Products.
Special categories of Personal Data	None	None
Subject matter and nature of the Processing	The technical functionality of the Subscription Services and provision of related technical support.	The provision of technical support in relation to the Products.
Purposes of the Processing	Providing the Subscription Services and technical support, including identifying errors reported by Authorized Users.	Providing technical support in relation to the Products, including identifying errors reported by Product Users.
Retention period	7 years	7 years
Sub-processor(s)	As set out at https://trust.qumulo.com/subprocessors	

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with clause 13 of the SCCs

The Irish Data Protection Commissioner.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

Qumulo has implemented the following technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Qumulo's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Qumulo's organization, monitoring and maintaining compliance with Qumulo's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Utilization of commercially available and industry standard encryption technologies for Covered Data that is:

   (a) a) being transmitted by Qumulo over public networks (i.e., the Internet) or when transmitted wirelessly; or

   (b) b) at rest, stored on local devices, in network storage, or in the cloud

4. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

5. Password controls designed to manage and control password strength, including controls prohibiting users from sharing passwords and requiring that Qumulo's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Qumulo's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

7. Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Qumulo facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Qumulo's possession.

9. Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Qumulo's technology and information assets.

10. Incident / problem management procedures designed to allow Qumulo to investigate, respond to, mitigate, and notify of events related to Qumulo's technology and information assets.

11. Network security controls that provide for the use of firewall systems, intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

1. EU SCCS

With respect to any transfers referred to in clause 13, the Standard Contractual Clauses shall be completed as follows:

1.1 Module Two will apply in the case of the Processing under clause 3(a)(i) of the DPA and Module Three will apply in the case of Processing under clause 3(a)(ii) of the DPA.

1.2 Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

1.3 Clause 9(a) option 2 (General written authorization) shall apply, and the time period to be specified is determined in clause 6.4 of the DPA.

1.4 The option in Clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.

1.5 With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that, option 1 will apply and the governing law will be the law of the Republic of Ireland.

1.6 In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of the Republic of Ireland.

1.7 For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority

1.8 For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 2 of the DPA contains the technical and organizational measures.

1.9 The specifications for Annex III of the Standard Contractual Clauses, are determined by clause 6.2 of the DPA. The Sub-processor's contact person's name, position and contact details will be provided by Qumulo upon request.

2. UK ADDENDUM

2.1 This paragraph 2 (*UK Addendum*) shall apply to any transfer of Covered Data from Customer (as data exporter) to Qumulo (as data importer), to the extent that:

(a) the UK Data Protection Laws apply to Customer when making that transfer; or

(b) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2:

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum.

"**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:

(a) the "Addendum EU SCCs" shall refer to the SCCs as they are incorporated into this Agreement in accordance with clause 13 and this Schedule 3;

(b) Table 1 of the Approved Addendum shall be completed with the details in paragraph A of Schedule 1;

(c) the "Appendix Information" shall refer to the information set out in Schedule 1 and Schedule 2

(d) for the purposes of Table 4 of the Approved Addendum, Qumulo (as data importer) may end this DPA, to the extent the Approved Addendum applies, in accordance with Section 19 of the Approved Addendum; and

(e) Section 16 of the Approved Addendum does not apply.

3. SWISS ADDENDUM

3.1 This Swiss Addendum will apply to any Processing of Covered Data that is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR.

3.2 Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

"**Addendum**" means this addendum to the Clauses;

"**Clauses**" means the Standard Contractual Clauses as incorporated into this DPA in accordance with clause 13 and as further specified in this Schedule 3; and

"**FDPIC**" means the Federal Data Protection and Information Commissioner.

(b) This Addendum shall be read and interpreted in a manner that is consistent with Swiss Data Protection Laws, and so that it fulfills the Parties' obligations under Article 16(2)(d) of the FADP.

(c) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Swiss Addendum has been entered into.

(e) In relation to any Processing of Personal Data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends and supplements the Clauses to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer; and

(ii) as standard data protection clauses approved, issued or recognized by the FDPIC for the purposes of Article 16(2)(d) of the FADP.

3.3 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 Changes to the Clauses for transfers exclusively subject to Swiss Data Protection Laws

To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.3(a)) the following amendments are made to the Clauses:

(a) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(b) Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer."

(c) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(d) References to Regulation (EU) 2018/1725 are removed.

(e) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(f) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

(g) Clause 17 is replaced to state:

"These Clauses are governed by the laws of Switzerland".

(h) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws will be resolved by the courts of Switzerland. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

3.5 Supplementary provisions for transfers of Personal data subject to both the GDPR and Swiss Data Protection Laws

(a) To the extent that the data exporter's Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" under both the Clauses and the Clauses as amended by paragraph 3.3(c) of this Addendum:

(i) for the purposes of Clause 13(a) and Part C of Annex I:

(A) the FDPIC shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer, or such transfer is an "onward transfer" as defined in the Clauses (as amended by paragraph 3.3 of this Addendum; and

(B) subject to the provisions of paragraph 2 of this Schedule 3 (UK Addendum), the supervisory authority identified in Schedule 1 shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent the GDPR applies to the data exporter's processing, or such transfer is an "onward transfer" as defined in the Clauses.

(b) the terms "European Union", "Union", "EU", and "EU Member State" shall not be interpreted in a way that excludes the ability of Data Subjects in Switzerland bringing a claim in their place of habitual residence in accordance with Clause 18(c) of the Clauses.

4. Transfers under the laws of other jurisdictions

4.1 With respect to any transfers of Personal Data referred to in clause 13.1(b) (each a "**Global Transfer**"), the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the Exporter Data Protection Laws.

4.2 For the purposes of any Global Transfers, the SCCs shall be deemed to be amended to the extent necessary so that they operate:

(a) for transfers made by the applicable data exporter to the data importer, to the extent the Exporter Data Protection Laws apply to that data exporter's Processing when making that transfer; and

(b) to provide appropriate safeguards for the transfers in accordance with the Exporter Data Protection Laws.

4.3 The amendments referred to in clause paragraph 4.2 include (without limitation) the following:

(a) references to the "GDPR" and to specific Articles of the GDPR are replaced with the equivalent provisions under the Exporter Data Protection Laws;

(b) reference to the "Union", "EU" and "EU Member State" are all replaced with reference to the jurisdiction in which the Exporter Data Protection Laws were issued (the "**Exporter Jurisdiction**");

(c) the "competent supervisory authority" shall be the applicable supervisory in the Exporter Jurisdiction; and

(d) Clauses 17 and 18 of the SCCs shall refer to the laws and courts of the Exporter Jurisdiction respectively.

4.4 Where, at any time during Qumulo's Processing of Covered Data under this DPA, a transfer mechanism other than the SCCs is approved under the Exporter Data Protection Laws with respect to transfers of Covered Data by Customer to Qumulo, the Parties shall promptly enter into a supplementary agreement that:

(a) incorporates any standard data protection clauses or another transfer mechanism formally adopted by the relevant authority in the Exporter Jurisdiction;

(b) incorporates the details of Processing set out in Schedule 1;

(c) shall, with respect to the transfer of Personal Data subject to the Exporter Data Protection Laws, take precedence over this DPA in the event of any conflict.

4.5 Where required under the Exporter Data Protection Laws, the relevant data exporter shall file a copy of the agreement entered into in accordance with paragraph 4.4 with the relevant national authority