For agreements completed prior to October 14, 2021.

DATA PRIVACY AGREEMENT

Seagate Technology LLC (“**Seagate**”) and you (“**Customer**”) (each a “**party**” and collectively the “**parties**”) have entered into a Lyve Services Agreement for Data Transfer Service (the “**Agreement**”) under which Seagate may Process Customer Personal Information (as defined below) in furtherance of providing certain services to the Customer (“**Services**”). This Data Privacy Agreement, including all schedules and exhibits attached hereto (this “**DPA**”), governs Seagate’s Processing of Customer Personal Information and shall form part of and be incorporated by reference into the Agreement and takes effect on the date of execution of the same (“**Effective Date**”).

The parties acknowledge and agree as follows:

1. **DEFINITIONS**

1.1 “**Affiliate**” means any entity which controls, is controlled by, or is under common control with the subject party, where “control” means ownership of or right to control greater than 50% of the voting securities of such entity.

1.2 “**Applicable Privacy Law(s)**” means all worldwide data protection and privacy laws and regulations, applicable to the Customer Personal Information in question, including where applicable: (i) EU Data Protection Law; (ii) all laws and regulations of the United States, including the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq ("**CCPA**"), as amended, superseded or updated from time to time; and (iii) applicable industry standards appropriate to the nature of the Customer Personal Information.

1.3 “**Data Privacy Breach**” means any confirmed breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of Customer Personal Information, or any other unauthorized Processing of Customer Personal Information.

1.4 “**EU Data Protection Law(s)**” means all data protection laws and regulations applicable to the European Union (“**EU**”) or the European Economic Area (“**EEA**”), including (a) the General Data Protection Regulation 2016/679 (“**GDPR**”); (b) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (c) applicable national implementations of (a) and (b); and (c) in respect

of the United Kingdom ("**UK**") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union).

1.5 "**Customer Personal Information**" means any data that is protected as "personal data", "personally identifiable information" or "personal information" under Applicable Privacy Law and processed by Seagate on behalf of Customer in connection with the Agreement.

1.6 "**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively (as amended, superseded or replaced from time to time).

1.7 "**Process**" or "**Processing**" means, without limitation, operations performed on Customer Personal Information, whether or not by automated means, such as collecting, recording, organizing, structuring, altering, using, accessing, disclosing, disseminating, copying, transferring, storing or otherwise retaining, deleting, aligning, combining, restricting, adapting, retrieving, consulting, destroying, or disposing of Customer Personal Information.

1.8 "**Sensitive Information**" means any of the following types of Customer Personal Information: (i) social security number, taxpayer identification number, passport number, driver's license number or other government-issued identification number; (ii) credit or debit card details or financial account number, with or without any code or password that would permit access to the account or credit history; or (iii) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political or philosophical beliefs, political party or trade union membership, background check information or judicial data such as criminal records or information on other judicial or administrative proceedings together with any Customer Personal Information of children protected under any child data protection laws, and any other information or combinations of information that falls within the definition of "special categories of data" under GDPR or any other applicable law relating to privacy and data protection.

1.9 "**Standard Clauses**" means the Standard Contractual Clauses for Processors issued by the European Commission on the basis of Article 26(4) of Directive 95/46/EC pursuant to Decision 2010/87/EU, in the form attached at Annex C (as amended, replaced or superseded from time to time in accordance with this DPA).

1.10 "**Sub-processor**" means any third party engaged by Seagate or by any other Sub-processor who will have access to, receive, or otherwise Process any Customer Personal Information.

1.11 "**Seagate Personnel**" means any Seagate employee, contractor, Sub-processor or agent whom Seagate authorizes to Process Customer Personal Information.

1.12 The terms "**Controller**," "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in EU Data Protection Law, and the terms "**Business**", "**Business Purpose**", "**Commercial Purpose**", "**Collect**", "**Consumer**", "**Service Provider**" and "**Sell**" shall have the meanings given to them in the CCPA.

1.13 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. DATA SECURITY AND PROTECTION

2.1 **Data Protection Roles**. The parties hereby acknowledge and agree that Customer is the Controller and Seagate is acting on behalf of the Customer as the Processor or Service Provider with respect to the Customer Personal Information, except where Customer acts as Processor of Customer Personal Information, in which case Seagate is a Sub-processor.

2.2 **Compliance with Laws**. Each Party shall comply with its obligations under Applicable Privacy Law(s) in respect of any Customer Personal Information it processes under this DPA. Any processing of Customer Personal Information under the Agreement shall be performed in accordance with Applicable Privacy Laws. However, Seagate is not responsible for compliance with any Applicable Privacy Law or local/industry standards which may apply to Customer or Customer's industry that is not generally applicable to Seagate as a service provider. Where Customer's specific use of the services and Applicable Privacy Law or local/industry standards requires Customer to enter into specific contractual arrangements and/or additional compliance steps or measures that extend beyond the provisions of this DPA, Customer is responsible for notifying Seagate at Corporate.Contracts@Seagate.com at least thirty (30) days prior to providing Seagate with Customer Personal Information subject to such requirements. Seagate will provide reasonable assistance to Customer in supporting its compliance with such requirements, and Seagate, in its entire discretion, may execute the necessary agreement(s) that extend to applicable Customer Personal Information covered under such provisions, without giving less effect to the provisions of this DPA. Customers may notify Seagate about such jurisdiction specific requests at the notice address for the Seagate contracting entity identified in the Agreement.

2.3 **Nondisclosure of Customer Personal Information**. Seagate shall not disclose Customer Personal Information in any manner for any purpose to any third party without obtaining prior written authorization from Customer, other than disclosures made in accordance with applicable law, to Sub-processors in accordance with Section 2.8 below, or otherwise in furtherance of providing the Services.

2.4 **Scope of Processing**. Seagate shall at all times: (i) process the Customer Personal Information solely for the purposes of providing the Services to Customer under the Agreement and in accordance with Customer's documented lawful instructions ("**Permitted Purposes**"); and (ii) not process Customer Personal Information for its own purposes or those of any third party. Seagate shall not (i) sell or disclose Personal Information for monetary or other valuable consideration; (ii) retain, use or disclose Personal Information for any purposes other than for the Permitted Purpose(s), including retaining, using or disclosing Personal Information for a commercial purpose other than performing the Services under the Agreement(s); or (iii) retain, use or disclose Personal Information outside the direct business relationship between Seagate and Customer. Seagate certifies that it understands and will comply with the requirements and restrictions set out in Section 2.4 and will comply with the requirements applicable to Service Providers under the CCPA.

2.5 **Processing Instructions**. The parties agree that the Agreement (including this DPA) sets out the Customer's complete and final instructions to Seagate in relation to the processing of Customer Personal Information. If Seagate is required by law to process the Customer Personal Information for any other purpose, Seagate will inform Customer of such requirement prior to the processing, unless and to the extent prohibited by law from doing so. Any changes to the Customer's instructions are subject to approval by the Parties (including additional costs for complying with new instructions).

2.6 **Customer Obligations**. Customer agrees that (i) it shall comply with its obligations under Applicable Privacy Laws in respect of its processing of Customer Personal Information and any processing instructions it issues to Seagate; and (ii) it has provided notice and obtained (or shall obtain) all consents (where required) and rights necessary under Applicable Privacy Laws for Seagate to process Customer Personal Information and provide the Services pursuant to the Agreement and this DPA; and (iii) it is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of personal data when in transit to and from the Service and taking any appropriate steps to securely encrypt or backup any personal data processed in connection with the Services. Customer shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Information from Data Privacy Breach and to preserve the security and confidentiality of personal data while in its dominion and control.

2.7 **Information Security Program**. Seagate will implement, maintain, monitor and, where necessary, update a comprehensive written information security program that contains appropriate administrative, technical, and physical safeguards to protect Customer Personal Information against anticipated threats or hazards to its security, confidentiality or integrity (such as unauthorized access, collection, use, copying, modification, disposal or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage or any other unauthorized form of Processing) ("**Information Security Program**"). Customer acknowledges that the Information Security Program is subject to technical progress and development and that Seagate may update or modify such program from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

2.8 **Restrictions on Sub-processors**. Seagate may disclose Customer Personal Information to Sub-processors as necessary to perform its Services for Customer, subject to the conditions set forth in this Section 2.8. By signing this DPA Customer hereby provides general written authorization for Seagate to engage Sub-processors to provide the Services. The Sub-processors currently engaged by Seagate and authorized by Customer are listed in Annex D to this DPA. Customer may subscribe for e-mail notifications of Sub-processor changes by subscribing at corporatecontracts@seagate.com with the following subject line *"Subscribe To Lyve Portal Agreement DPA Sub-Processor Update Alerts"*. Seagate shall notify Customer if it changes Sub-processors prior to any such changes. Customer may object in writing to the appointment of each such sub-processor on reasonable grounds (e.g., if making Customer Personal Information available to the Sub-processor may violate Applicable Privacy Law or weaken the protections for such Customer Personal Information) by notifying Seagate promptly in writing within **ten (10) calendar days** of receipt of Seagate notice in accordance with this Section 2.8. Such notice shall explain the reasonable grounds for the objection and the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If Customer does not object to the proposed Sub-processor within **ten (10) calendar days** of receipt of notice, the Sub-processor is deemed to have been approved. Seagate may in its sole discretion, remove the Sub-processor from the list. In the event a Sub-processor is removed by Seagate, Seagate will be provided a reasonable amount of time to replace the Sub-processor.

2.9 **Sub-processor Performance**. Where a Sub-processor fails to fulfil its data protection obligations or is removed by Seagate, Seagate shall remain fully liable to Customer for the performance of the Sub-processor's obligations. If Seagate cannot perform the obligations without the Sub-processor, then Seagate may terminate any applicable Agreement(s) between the parties and/or their Affiliates without cost or liability owed to Customer.

2.10 **Obligations of Seagate Personnel and Sub-processors**. Seagate shall ensure that any persons authorized to Process Customer Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Where Seagate engages a Sub-processor for carrying out specific Processing activities on behalf of Customer, Seagate will enter into a written agreement with the Sub-processor containing data protection obligations that impose at a minimum, data privacy, protection and information security requirements on the Sub-processor for the duration of the Processing that require the Sub-processor to protect the Customer Personal Information to the standard required by Applicable Privacy laws.

2.11 **Notice of Requests or Complaints**. Unless prohibited by law, Seagate shall notify Customer of any request or complaint received by Seagate relating to the Processing of Customer Personal Information, including:

(a) requests from a Data Subject to exercise one of their rights provided by Applicable Privacy Laws, including but not limited to a request for data portability, to access, change, delete, or restrict, and similar requests; or

(b) complaints or allegations that the Processing infringes on a Data Subject's rights.

2.12 **Customer Responses to Data Subject Requests**. Taking into account the nature of the Processing, Seagate shall assist Customer by appropriate technical and organizational measures, insofar as it is possible, for the fulfillment of Customer's obligations to respond to requests from Data Subjects to exercise their rights at Customer's expense. Seagate will promptly inform Customer in writing if it receives: (i) a request from a data subject concerning the processing of Customer Personal Information except for CCPA requests where Seagate shall inform the requestor that the request cannot be acted upon because the request has been sent to a service provider, as defined in the CCPA; or (ii) a complaint, communication, or request relating to Customer's obligations under Applicable Privacy Laws. Except as noted in (i) regarding CCPA requests, Seagate shall not respond to such request, complaint or communication directly (except to direct the data subject to contact the Customer) without Customer's prior authorization, unless legally compelled to do so.

2.13 **Requests for Disclosure**. Customer acknowledges that Seagate may be required to disclose, without advance notice or Customer consent, Customer Personal Information to authorities in connection with any investigation, audit or inquiry in connection with the services. Unless prohibited by law, Seagate will use commercially reasonable efforts to notify Customer if Seagate receives any document requesting or purporting to compel the disclosure of Customer Personal Information (such as oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, or other similar

requests or processes). Seagate shall exercise commercially reasonable efforts to prevent and limit any disclosure and to preserve the confidentiality of Customer Personal Information.

2.14 **Cooperation**. At Customer's expense, Seagate shall provide reasonable assistance to Customer in meeting its obligations under Applicable Privacy Laws regarding the security of Customer Personal Information and fulfilling privacy and data protection impact assessments (as reasonably required) and related consultations of Supervisory Authorities.

2.15 **Notice of Potential Violations or Inability to Comply**. Seagate shall notify Customer if:

(a) Seagate has reason to believe that any instructions from Customer regarding Processing of Customer Personal Information would violate applicable law;

(b) Seagate has reason to believe that it is unable to comply with any of its obligations under this DPA or Applicable Privacy Laws and it cannot cure this inability to comply within a reasonable timeframe; or

(c) Seagate becomes aware of any circumstances or changes in applicable law that are likely to prevent it from fulfilling its obligations under this DPA.

3. **DATA TRANSFERS**

3.1 **Transfer Mechanisms**. To the extent Seagate is a recipient of and processes Personal Data protected by European Data Protection Law outside of the EEA in a country that is not recognized as providing an adequate level of protection for personal data (within the meaning of applicable European Data Protection Law), the parties agree the following:

(a) **Standard Contractual Clauses**: Seagate agrees to abide by and process such Personal Data in compliance with the Standard Contractual Clauses ("SCCs"), which are incorporated into and form a part of this DPA. The parties agree that (i) purely for the purposes of the descriptions in the SCCs Seagate is the "data importer" and Customer is "data exporter" (notwithstanding that Customer may itself be located outside Europe and/or is acting as a processor on behalf of a third party controller); and (ii) it is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict; and

(b) **Alternative Transfer Mechanism**: To the extent Seagate adopts an alternative data export mechanism (including any new version of or successor to the SCCs or Privacy Shield adopted pursuant to applicable European Data Protection Law) for the transfer of Personal Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer

Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred) and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism. In addition, if and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders or determines (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer such Personal Data, Customer acknowledges and agrees that Seagate may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such Personal Data.

(c) UK Data Transfers: For the avoidance of doubt, when the European Union law ceases to apply to the UK upon the UK's withdrawal from the European Union and until such time as UK is deemed to provide adequate protection for Personal Data (within the meaning of applicable European Data Protection Law) then to the extent Seagate processes (or causes to be processed) any Personal Data protected by European Data Protection Law applicable to EEA and Switzerland in the United Kingdom, Seagate shall process such Personal Data in compliance with the SCCs or any applicable Alternative Transfer Mechanism implemented in accordance with Section 3 of this DPA.

3.2 **Transfers out of countries with data export requirements**. If any Applicable Privacy Laws require that further steps be taken in relation to any applicable data export restriction to permit the transfer of Customer Personal Information to Seagate (including its Sub-processors), Customer will comply with such data protection requirements including acquiring requisite consents or executing any applicable data transfer agreements (e.g. standard contractual clauses) or an alternative solution to ensure the appropriate safeguards are in place for such transfer.

4. COMPLIANCE AND ACCOUNTABILITY

4.1 **Audit**. No more than once every **twelve (12) months**, Customer may request Seagate make available to Customer information strictly necessary to demonstrate compliance with Article 28 of the GDPR in relation to the Processing of Customer Personal Information. Seagate shall allow for and contribute to audits by Customer or an independent third-party auditor mandated by Customer, at Customer's expense. Any such independent third-party auditor must be approved by Seagate (except if such third party is a competent Supervisory Authority). The auditor must execute a written confidentiality agreement acceptable to Seagate or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

4.2 **Audit Scope**. To request an audit, Customer must provide Seagate **thirty (30) calendar days** prior written notice and submit to Seagate a proposed audit plan describing the proposed scope, duration, and start date of the audit. Seagate will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Seagate or Seagate customer's security, privacy, employment or other relevant policies). Seagate will work cooperatively with Customer to agree on a final audit plan.

4.3 **Audit Report**. Customer will provide Seagate any audit reports generated in connection with any audit, unless otherwise prohibited by Applicable Privacy Laws or otherwise instructed by a Supervisory Authority. Customer may only use the audit reports for the purposes of meeting Customer's regulatory audit requirements and/or for confirming compliance with the requirements of this DPA. The audit reports, including any informative information provided by Seagate for the audit, are Seagate's Confidential Information.

5. SEAGATE RESPONSIBILITIES AFTER A DATA PRIVACY BREACH

5.1 **Notification of Data Privacy Breach**. Seagate shall notify Customer in writing of a Data Privacy Breach without undue delay, and shall:

(a) investigate or provide reasonable assistance in the investigation of the Data Privacy Breach;

(b) provide Customer with information about the Data Privacy Breach, and promptly provide additional relevant information as it becomes available; and

(c) take commercially reasonable steps to contain the Data Privacy Breach, mitigate the effects of the Data Privacy Breach, or assist Customer in doing so at Customer's expense.

5.2 **Notification Considerations**. notification of or response to a Data Privacy Breach under this paragraph ("Data Privacy Breach Response") will not be construed as an acknowledgment by Seagate of any fault or liability with respect to the Data Privacy Breach.

5.3 **Communications**. Seagate shall not issue any communications related to a Data Privacy Breach, in any manner that would identify, or is reasonably likely to identify or reveal the identity of, Customer, without Customer prior approval, unless otherwise required by law.

5.4 **Preservation of Evidence**. Seagate shall maintain an incident response plan. Following discovery of a Data Privacy Breach, Seagate shall preserve available evidence related to the Data Privacy Breach and maintain a clear chain of command according to Seagate's incident response plan.

6. RETURN AND SECURE DELETION OF CUSTOMER PERSONAL INFORMATION

6.1 **Return and Deletion of Customer Personal Information.** Upon the earlier of (a) request by Customer or (b) the expiration or earlier termination of the agreement(s) between the parties and/or their Affiliates related to the Processing of Customer Personal Information, at Customer's direction, Seagate shall, and shall direct its Sub-processors to, export the Customer Personal Information or provide Customer, or its third-party designee, with the ability to export all Customer Personal Information in a machine readable and interoperable format. Each party shall identify a contact person to migrate the Customer Personal Information and shall work promptly, diligently, and in good faith to facilitate a timely transfer. Within **90 days** after Seagate (a) completes migration of Customer Personal Information, or (b) Customer informs Seagate of its election to not migrate the Customer Personal Information, Seagate and Sub-processors shall securely destroy all Customer Personal Information and overwrite with new data or otherwise destroy the Customer Personal Information through an approved sanitization method.

6.2 **Deletion Obligations**. Notwithstanding Section 6.1, regardless of whether Customer directs Seagate to return Customer Personal Information, Customer may be required to delete Customer Personal Information off the services upon the expiration or earlier termination of the agreement(s) between the parties and/or their Affiliates related to the Processing of Customer Personal Information. Should Customer choose to intake or migrate Customer Personal Information into another Seagate service including but not limited to Seagate Lyve Cloud, Customer acknowledges that Seagate may, upon a successful intake or migration of such data, delete or otherwise dispose of any Customer Personal Information stored in the original service. Customer acknowledges that due to the nature of the service Seagate will not have technical access to the data without additional permissions, in order to ensure continuity of security.

6.3 **Destruction of Customer Personal Information**. If Seagate disposes of any paper, electronic or other record containing Customer Personal Information, Seagate will do so by taking all reasonable steps (based on the sensitivity of the Customer Personal Information) to destroy Customer Personal Information by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying the Customer Personal Information in such records to make it unreadable, unreconstructable and indecipherable. If Seagate decommissions or otherwise retires a hard drive that contains a copy of Customer Personal Information then Seagate shall securely shred or destroy the drive rendering the Customer Personal Information unreadable and destroyed in accordance with NIST 800-88, revision 1.

7. MISCELLANEOUS

7.1 **Term**. This DPA will remain in effect until (i) there is no other active agreement(s) between the parties and (ii) Seagate has ceased to have custody or control of or access to any Customer Personal Information.

7.2 **Order of Precedence**. The Agreement remains unchanged and in full force and effect. In case of discrepancies between this DPA and any agreement(s) between the parties and/or their Affiliates, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses (where applicable); then (b) this DPA; and then (c) the main body of the Agreement. This DPA shall not limit or restrict, but shall only be deemed to supplement the Standard Contractual Clauses.

7.3 **Updates**. The parties will reasonably cooperate to update this DPA by mutual written agreement as needed to ensure compliance with applicable laws and regulations.

7.4 **Service Data**. Notwithstanding anything to the contrary in the Agreement (including this DPA), Seagate shall have a right to collect, use and disclose data relating to the use, support and/or operation of the Services ("**Service Data**") for its legitimate business purposes, such as billing, account management, technical support, and product development. To the extent any such Service Data is considered Customer Personal Information under Applicable Privacy Laws, Seagate shall be responsible for and shall process such data in accordance with the Seagate Privacy Policy (the most current version of which is located at https://www.seagate.com/legal-privacy/) (as updated from time to time) and Applicable Privacy Laws. For the avoidance of doubt and except for this Section 7.4, the terms of this DPA shall not apply to Service Data.

7.5 **Third Party Beneficiaries**. Seagate's Affiliates are intended third-party beneficiaries of this DPA; and may enforce the terms of this DPA as if each was a signatory to this DPA. Seagate also may enforce the provisions of this DPA on behalf of its Affiliates, instead of its Affiliates separately bringing a cause of action against Customer.

7.6 **Disclosure to Supervisory Authority or Regulatory Body**. Customer acknowledges that Seagate may disclose this DPA (including the SCCs) and any relevant privacy provisions in the Agreement to the Federal Trade Commission, a European data protection authority, or any other US or European judicial or regulatory body upon their request.

7.7 **Severance**. If any provision in this DPA is ineffective or void, this will not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith.

7.8 **Counterparts**. This DPA may be signed by electronic signature, and such electronic signature shall be treated as an original, including for evidentiary purposes. This DPA may be signed in two or more counterparts, none of which needs to contain the signatures of both of the parties, and each of which will be deemed to be an original, and all of which taken together will constitute one and the same instrument.

7.9 **Interpretation**. The headings in this DPA are for reference only and will not affect the interpretation of this agreement.

7.10 **Liability**. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) whether in contract, tort (including negligence) or under any other theory of liability, shall be subject to the limitations and exclusions of liability in (or incorporated by reference into) the Agreement to the maximum extent permitted by Applicable Privacy Laws, provided that such limits shall not apply to either party's liability arising under the Standard Contractual Clauses.

7.11 **Choice of Law**. This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Privacy Laws.

ANNEX A

DETAILS OF PROCESSING

Duration

The duration of the Agreement plus the period from the expiry of the Agreement until the deletion of the Customer Personal Information by Customer or Seagate in accordance with the Agreement.

Data Exporter

Customer, a user of Seagate hardware products and software solutions and services to support its business processes.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Seagate a provider of hardware products and software solutions and services to support business processes of various industry segments.

Categories of data subjects

Customer may submit personal data to Seagate, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects:

- The Customer Personal Information transferred may concern the following categories of data subjects:
- Past and present employees, advisors, consultants, suppliers, contractors, subcontractors and agents of the Customer;
- Past and present partners of the Customer, and their employees, partners, advisors, consultants, suppliers, contractors, subcontractors and agents; and
- Past and present customers of the Customer, and their employees, partners, advisors, consultants, suppliers, contractors, subcontractors and agents.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data provided by Customer, provided on behalf of Customer, or collected by Seagate in connection with the services.

Special categories of data (if appropriate)

Data provided by Customer, provided on behalf of Customer, or collected by Seagate in connection with the services.

Processing operations

Customer Personal Information will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

(i) Storage and other processing necessary to provide, maintain and improve the Services provided to Customer pursuant to the Agreement; and/or

(ii) Disclosures in accordance with the Agreement and/or as compelled by applicable law

ANNEX B

SECURITY MEASURES

Seagate will implement, maintain, monitor and, where necessary, update a comprehensive written information security program that contains appropriate administrative, technical, and physical safeguards to protect Customer Personal Information against anticipated threats or hazards to its security, confidentiality or integrity (such as unauthorized access, collection, use, copying, modification, disposal or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage or any other unauthorized form of processing) ("Information Security Program").

Customer acknowledges that the Information Security Program is subject to technical progress and development and that Seagate may update or modify such program from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Lyve Services purchased by Customer.

Seagate does not review, edit, or take any responsibility for data, content or material created, stored or made accessible through the Lyve Services, and, as a result, does not accept responsibility from Customer for any resulting damages or liabilities arising therefrom.

ANNEX C

STANDARD CONTRACTUAL CLAUSES

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Customer

(the data exporter)

And

Name of the data importing organization:

Seagate Technology LLC, signing on behalf of Affiliates and subsidiaries.

Address: 47488 Kato Road, Fremont, CA 94538
Tel. +1 510-661-1000; e-mail:data.protection.officer@seagate.com

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’* and *‘supervisory authority’* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) ‘*the data exporter’* means the controller who transfers the personal data;

(c) *‘the data importer’* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his

instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data

exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could

be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The details of the transfer are covered in Annex A of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures implemented by the data importer are described in Annex B of the DPA.

ANNEX D

SUBPROCESSORS

Disclosure of Personal Information

In furtherance of providing Services to Customer, Seagate discloses Personal Information to its affiliate Seagate Technology LLC, located in the United States.