DATA PRIVACY AGREEMENT

The Seagate contracting party identified in your Lyve Services agreement ("**Seagate**") and you ("**Company**") (each a "**party**" and collectively the "**parties**") have entered into a Lyve Services agreement (the "**Agreement**") under which Seagate may Process Company Personal Information (as defined below) in furtherance of providing certain services to the Company ("**Services**"). This Data Privacy Agreement, including all schedules and exhibits attached hereto (this "**DPA**"), governs Seagate's Processing of Company 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 Company 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the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq ("**CCPA**"), as amended, superseded or updated from time to time; and (iii) applicable industry standards appropriate to the nature of the Company Personal Information.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 Company Personal Information, or any other unauthorized Processing of Company 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 ("**EU GDPR**" or "**GDPR**"); (b) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "**UK GDPR**"); (c) the Swiss Federal Data Protection Act of 19 June 1992

and its corresponding ordinances ("**Swiss DPA**"); (d) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (e) applicable national implementations of (a),(b), and (c).

1.5 "Company 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 Company in connection with the Agreement, as more particularly described in Annex A of this DPA.

1.6 "Model Clauses" or "**SCCs**" means (i) where the GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses for Processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs") (as amended, superseded or updated from time to time).

1.7 "**Process**" or "**Processing**" means, without limitation, operations performed on Company 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 Company Personal Information.

1.8 "Restricted Transfer" means: (i) where the GDPR applies, a transfer of Company Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Company Personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where Swiss DPA applies, a transfer of Company Personal Data from Switzerland to any other country which is not based on an adequacy decision recognized under Swiss data protection law.

1.9 "Sensitive Information" means any of the following types of Company 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 Company 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.

1.10 “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 Company Personal Information.

1.11 “Seagate Personnel” means any Seagate employee, contractor, Sub-processor or agent whom Seagate authorizes to Process Company 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**”, “**Services 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 Company is the Controller or Business, and Seagate is acting on behalf of the Company as the Processor or Service Provider with respect to the Company Personal Information, except where Company acts as Processor of Company 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 Company Personal Information it processes under this DPA. Any processing of Company 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 Company or Company's industry that is not generally applicable to Seagate as a service provider. Where Company's specific use of the services and Applicable Privacy Law or local/industry standards requires Company to enter into specific contractual arrangements and/or additional compliance steps or measures that extend beyond the provisions of this DPA, Company is responsible for

notifying Seagate at least thirty (30) days prior to providing Seagate with Company Personal Information subject to such requirements. Seagate will provide reasonable assistance to Company in supporting its compliance with such requirements, and Seagate, in its entire discretion, may execute the necessary agreement(s) that extend to applicable Company Personal Information covered under such provisions, without giving less effect to the provisions of this DPA. Company 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 Company Personal Information. Seagate shall not disclose Company Personal Information in any manner for any purpose to any third party without obtaining prior written authorization from Company, 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 Company Personal Information solely for the purposes of providing the Services to Company under the Agreement and in accordance with Company's documented lawful instructions (“Permitted Purposes”); and (ii) not process Company Personal Information for its own purposes or those of any third party. Seagate shall not (i) sell or disclose Company Personal Information for monetary or other valuable consideration; (ii) retain, use or disclose Company Personal Information for any purposes other than for the Permitted Purpose(s), including retaining, using or disclosing Company Personal Information for a commercial purpose other than performing the Services under the Agreement(s); or (iii) retain, use or disclose Company Personal Information outside the direct business relationship between Seagate and Company. 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 Company's complete and final instructions to Seagate in relation to the processing of Company Personal Information. If Seagate is required by law to process the Company Personal Information for any other purpose, Seagate will inform Company of such requirement prior to the processing, unless and to the extent prohibited by law from doing so. Any changes to the Company's instructions are subject to approval by the Parties (including additional costs for complying with new instructions).

2.6 Company Obligations. Company agrees that (i) it shall comply with its obligations under Applicable Privacy Laws in respect of its processing of Company 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 Company 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 Company Personal Information when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Company Personal Information processed in connection with the Services. Company shall implement and maintain appropriate technical and organizational security measures designed to protect Company Personal Information from Data Privacy Breach and to preserve the security and confidentiality of Company Personal Information 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 Company 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**"). Company 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 Company.

2.8 Restrictions on Sub-processors. Seagate may disclose Company Personal Information to Sub-processors as necessary to perform its Services for Company, subject to the conditions set forth in this Section 2.8. By signing this DPA Company 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 Company are listed in Annex C to this DPA. Company may subscribe for e-mail notifications of Sub-processor changes by subscribing at corporatecontracts@seagate.com with the following subject line "Subscribe to Lyve Cloud Data Privacy Agreement Sub-Processor Update Alerts". Seagate will provide at least **fifteen (15) calendar days** prior written notice to Company of the engagement of

any new Sub-Processor. Company may object in writing to the appointment of each such Sub-processor on reasonable grounds (e.g., if making Company Personal Information available to the Sub-processor may violate Applicable Privacy Law or weaken the protections for such Company Personal Information) by notifying Seagate promptly in writing within **ten (10) calendar days** of receipt of Seagate's 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. 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. If Company does not object to the proposed Sub-processor within **ten (10) calendar days** of receipt of Seagate's notice, the Sub-processor is deemed to have been approved.

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 Company 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 Company.

2.10 Obligations of Seagate Personnel and Sub-processors. Seagate shall ensure that any persons authorized to Process Company 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 Company, 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 Company Personal Information to the standard required by Applicable Privacy laws.

2.11 Notice of Requests or Complaints. Unless prohibited by law, Seagate shall notify Company of any request or complaint received by Seagate relating to the Processing of Company 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 Company Responses to Data Subject Requests. Taking into account the nature of the Processing, Seagate shall assist Company by appropriate technical and organizational measures, insofar as it is possible, for the fulfillment of Company's obligations to respond to requests from Data Subjects to exercise their rights at Company's expense. Seagate will promptly inform Company in writing if it receives: (i) a request from a data subject concerning the processing of Company 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 Company'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 Company) without Company's prior authorization, unless legally compelled to do so.

2.13 Requests for Disclosure. Company acknowledges that Seagate may be required to disclose, without advance notice or Company consent, Company 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 Company if Seagate receives any document requesting or purporting to compel the disclosure of Company 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 Company Personal Information.

2.14 Cooperation. At Company's expense, Seagate shall provide reasonable assistance to Company in meeting its obligations under Applicable Privacy Laws regarding the security of Company 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 Company if:

(a) Seagate has reason to believe that any instructions from Company regarding Processing of Company 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 International Transfers. Company hereby consents to Seagate transferring and Processing any Company Personal Information in or to a territory other than the territory in which the Company Personal Information was first collected provided that Seagate takes all such measures as are necessary to ensure such transfer and Processing is in compliance with Applicable Privacy Law and this DPA (including such measures as may be communicated by Company to Seagate from time to time).

3.2 Transfer Mechanisms. The parties agree that where transfer of Company Personal Information from Company to Seagate is a Restricted Transfer, it will be subject to the transfer mechanisms listed below:

(a) Model Clauses. The parties agree that the Restricted Transfer shall be subject to the appropriate Model Clauses, which are automatically incorporated by reference and form an integral part of this DPA, as follows:

(1) In relation to Company Personal Information that is protected by the GDPR, the EU SCCs will apply as follows:

(a) Module Two and Three as appropriate will apply;

(b) in Clause 7, the optional docking clause shall apply;

(c) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be fifteen (15) days;

(d) in Clause 11, the optional language will not apply;

(e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by English law;

(f) in Clause 18(b), disputes shall be resolved before the courts of England, UK;

(g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA; and

(h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA.

(2) In relation to data that is protected by the UK GDPR, the EU SCCs as implemented in accordance with paragraph (1) above will apply provided that:

(a) any references in the EU SCCs to "Directive 95/46/EC" or “Regulation (EU) 2016/679” shall be interpreted as references to the UK GDPR; references to specific Articles of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK GDPR; references to “EU”, “Union” and “Member State law” are all replaced with “UK”; Clause 13(a) and Part C of Annex II of the EU SCCs are not used; references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the Information Commissioner and the courts of England and Wales; Clause 17 of the EU SCCs is replaced to state that “The Clauses are governed by the laws of England and Wales” and Clause 18 of the EU SCCs is replaced to state “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts”;

(b) to the extent and for so long as the EU SCCs as implemented in accordance with paragraph 2(A) above cannot be used to lawfully transfer Company Personal Information protected by the UK DPA to Supplier, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to such transfers; and

(c) for the purposes of the UK SCCs (where applicable) the relevant Annexes/ Appendices of the UK SCCs shall be deemed completed using the information contained in Annex A and Annex B of this DPA.

(3) In relation to Company Personal Information that is protected by the Swiss DPA, the EU SCCs as implemented in accordance with paragraph (1) above will apply provided that:

(a) references in the EU SCCs to “Regulation (EU) 2016/679” or the “GDPR” shall be interpreted as references to the Swiss Federal Act on Data Protection (FADP);

(b) references to “EU”, “Union” and “Member State law” shall be interpreted as references to Switzerland and to Swiss law, as the case may be;

(c) the term ’member state’ shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland);

(d) the EU SCC clauses should be interpreted as protecting the data of legal entities until the entry into force of the revised FADP; and

(e) references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner (FDPIC) and competent courts in Switzerland.

(4) In the event that any provision of this Agreement or this DPA contradicts, directly or indirectly, the Model Clauses, the Model Clauses shall prevail.

(b) Alternative Transfer Mechanism: To the extent Seagate adopts an alternative data export mechanism (including any new version of or successor to the SCCs adopted pursuant to applicable EU 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 Company agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to 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 Company Personal Data, Company acknowledges and agrees that Seagate may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such Company Personal Data.

3.3 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 Company Personal Information to Seagate (including its Sub-processors), Company 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**, Company may request Seagate make available to Company information strictly necessary to demonstrate

compliance with Article 28 of the GDPR in relation to the Processing of Company Personal Information. Seagate shall allow for and contribute to audits by Company or an independent third-party auditor mandated by Company, at Company'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, Company 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 Company with any concerns or questions (for example, any request for information that could compromise Seagate or Seagate Affiliate's security, privacy, employment or other relevant policies). Seagate will work cooperatively with Company to agree on a final audit plan.

4.3 Audit Report. Company 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. Company may only use the audit reports for the purposes of meeting Company'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 Company in writing of a confirmed Data Privacy Breach without undue delay, and shall:

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

(b) provide Company 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 Company in doing so at Company'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, Company, without Company 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 COMPANY PERSONAL INFORMATION

6.1 Return and Deletion of Company Personal Information. Upon the earlier of (a) request by Company or (b) the expiration or earlier termination of the agreement(s) between the parties and/or their Affiliates related to the Processing of Company Personal Information, at Company's direction, Seagate shall, and shall direct its Sub-processors to, export the Company Personal Information or provide Company, or its third-party designee, with the ability to export all Company Personal Information in a machine readable and interoperable format. Each party shall identify a contact person to migrate the Company Personal Information and shall work promptly, diligently, and in good faith to facilitate a timely transfer. Within **30 days** after Seagate (a) completes migration of Company Personal Information, or (b) Company informs Seagate of its election to not migrate the Company Personal Information, Seagate and Sub-processors shall securely destroy all Company Personal Information and overwrite with new data or otherwise destroy the Company Personal Information through an approved sanitization method.

6.2 Deletion Obligations. Notwithstanding section 6.1, regardless of whether Company directs Seagate to return Company Personal Information, Seagate may be required to delete Company 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 Company Personal Information. Should Company choose to intake or migrate Company Personal Information into another Seagate service including but not limited to Seagate Lyve Services, Company acknowledges that Seagate may, upon a

successful intake or migration of such data, delete or otherwise dispose of any Company Personal Information stored in the original service. Company 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 Company Personal Information. If Seagate disposes of any paper, electronic or other record containing Company Personal Information, Seagate will do so by taking all reasonable steps to destroy Company Personal Information by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying the Company 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 Company Personal Information then Seagate shall securely shred or destroy the drive rendering the Company 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 Company 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 Company 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 Company.

7.6 Disclosure to Supervisory Authority or Regulatory Body. Company 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

DATA PROCESSING DESCRIPTION

A. LIST OF PARTIES

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

Data exporter(s):

COMPANY

Contact Details: As specified in the Agreement. The email address(es) Company designates in Company's account via its notification preferences.

Activities relevant to the transfer: Company utilizes the Lyve Service(s) specified in the Agreement and is responsible for use of the Lyve Service(s) in accordance with applicable documentation.

Signature and date: By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data exporter Role: The data exporter's role is set forth in Section 2.1 (Data Protection Roles) of the DPA.

Data importer(s):

SEAGATE

Contact Details: As specified in the Agreement. The Seagate Privacy Team may be contacted at data.protection.officer@seagate.com.

Activities relevant to the transfer: Seagate Processes Company Personal Information for the subject matter specified under the Agreement and until the Agreement terminates or expires, unless otherwise agreed upon by the parties in writing. The subject matter is determined by the Lyve Service(s) to which Company subscribes and the data which Company uploads to the Lyve Service(s).

Signature and date: By entering into the Agreement, data importer is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data importer Role: The data importer's role is set forth in Section 2.1 (Data Protection Roles) of the DPA.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

Categories of data subjects whose personal data is transferred

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

- Past and present employees, advisors, consultants, suppliers, contractors, subcontractors, and agents of the Company;
- Past and present business partners of the Company, and their employees, partners, advisors, consultants, suppliers, contractors, subcontractors, and agents; and
- Past and present customers of the Company, and their employees, partners, advisors, consultants, suppliers, contractors, subcontractors, and agents.

Categories of personal data transferred

Company may submit Company Personal Information to Seagate, the extent of which Company determines and controls in its sole discretion and may include personal data provided by Company, provided on behalf of Company, or collected by Seagate in connection with the Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Company may submit sensitive data to Seagate, the extent of which Company determines and controls in its sole discretion and may include sensitive data provided by Company, provided on behalf of Company, or collected by Seagate in connection with the Services. The safeguards Seagate implements are as described in Annex II.

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

Company determines and controls in its sole discretion the frequency of the transfer of personal data by Company to Seagate and Company conducts it in accordance with the Agreement (including this DPA).

Nature of the processing

Seagate will process Company Personal Information solely for the purposes of providing the Services to Company under the Agreement (including this DPA).

Purpose(s) of the data transfer and further processing

Company will transfer Company Personal Information to Seagate solely for the purposes of receiving the Services under the Agreement (including this DPA), including:

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

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

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

Seagate will retain Company Personal Information transferred by Company to Seagate in accordance with the Agreement (including this DPA) and in accordance with Company's documented lawful instructions.

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

Not applicable.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, is either (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to the processing of Company Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to the processing of personal data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

ANNEX B

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

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

Seagate implements, maintains, monitors and, where necessary, updates its comprehensive written information security program. Seagate's information security program contains administrative, technical, and physical safeguards to protect Company 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”).

Seagate has a separate and dedicated Information Security team that manages Seagate's Information Security Program. This team facilitates and supports independent audits and assessments performed by third parties. Company 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 Company.

Seagate does not review or edit, data, content, or material created, stored, or made accessible through the Lyve Services.

The following measures are in place to protect the Company Personal Data handled by Lyve Cloud Services and Lyve Mobile Services (collectively the “Lyve Services”):

Encryption of personal data: Measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- Seagate has implemented robust security measures to ensure Company data remains protected, including AES-256-GCM encryption at-rest for Lyve Cloud Services and TCG Enterprise, SED AES-256-bit encryption at rest for Lyve Mobile Services and support for encryption in-transit.
- A key security feature of the Lyve Services is that Seagate encrypts all data before storing it, regardless of whether it is encrypted at the source. There is no option to dial back the protection. When Company chooses to end its tenancy with Lyve Services, its data will be securely erased.
- Third-party data centers host Lyve Cloud Services, ensuring the highest class of data center availability and access. By design, data encryption cannot be disabled within Lyve Cloud Services. This means data is always encrypted at rest and in flight. Further, ransomware protection safeguards data from malicious attacks while object immutability protects data from accidental manipulation or deletion

Measures for ensuring ongoing Confidentiality, integrity, availability and resilience of processing systems and services:

- **Confidentiality:** Measures ensuring that information is accessed only by an authorized person and to prevent intrusion by unauthorized persons into systems and applications used for the processing of personal data.
    - Seagate has a dedicated access control policy.
    - Differentiated rights system based on security groups and access control lists.
    - Password policy, including guidelines for handling passwords.
    - Passwords require a defined minimum complexity. Initial passwords must be changed after the first login.
    - Access right management including authorization concept, implementation of access restrictions, implementation of the “need-to-know” principle, managing of individual access rights.
    - Training and confidentiality agreements for internal staff and external staff.
    - Network separation.
    - Authorization requests are tracked, logged, and audited on a regular basis.
    - Removal of access for employees upon termination or change of employment.
    - Account provisioning and de-provisioning processes.
    - Segregation of responsibilities and duties to reduce opportunities for unauthorized or unintentional modification or misuse.
    - Confidentiality requirements imposed on employees.
    - Mandatory security training for employees, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and overall security responsibilities inside and outside of Seagate.
    - Non-disclosure agreements with third parties.
    - Separation of networks based on trust levels.
- **Integrity:** Measures ensuring that Company Personal Information cannot be read, copied, modified, or removed without authorization during electronic transmission or transport, and that it is possible to check and establish whether and by whom data have been input into data processing systems, modified or removed.
    - Logging authentication and monitored logical system access.
    - Logging of data access including, but not limited to access, modification, entry and deletion of data.

        - Documentation of data entry rights and logging security related entries.
    - **Availability and resilience:** Measures that reduce the risk to Company Personal Information from accidental destruction or loss due to internal or external influences and ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

Measures for ensuring the ability to restore the availability and access to the Lyve Cloud Services system in a timely manner in the event of a physical or technical incident: Measures that ensure the possibility to quickly restore the system in the event of a physical or technical incident.

- Continuity planning and disaster recovery plan.
- Disaster recovery processes to restore processes.
- Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents.

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures of the Lyve Cloud Services in order to ensure the security of the processing:

- The monitoring and logging of activities chronicles events and generates evidence. Production and other critical systems produce event logs recording user activities, exceptions, faults, and information security events.
- Only authorized Seagate employees can access all logs and access controls are in place to prevent unauthorized access.
- Seagate protects log information against tampering and unauthorized access. This includes safeguarding the controls against unauthorized changes to log information and operational problems.

Measures for user identification and authorisation:

- Procedures are in place to capture and log information related to the interaction of systems, applications, and user accounts.
- Access to program source code and associated items (such as designs, specifications, verification, and validation plans) is restricted in order to prevent the introduction of unauthorized functionality and to avoid

unintentional changes, as well as to maintain the confidentiality of intellectual property.

- A formal user registration and de-registration process for managing identifications is implemented to assign access rights. This includes issuing unique user identifications to identify the person authorized access to the Lyve Services (shared identifications are not permitted) and immediately disabling or removing identifications when someone terminates employment or when a contractor/vendor terminates a contract, or no longer requires access.
- Control of the allocation of secret authentication information (e.g., passwords, cryptographic keys, hardware tokens, or smart cards) must be maintained through a formal process that requires users to acknowledge, as part of their terms and conditions of employment, to keep this information confidential.

Measures for the protection of Data during transmission to Lyve Cloud Services:

- Lyve Cloud Services has implemented robust security measures to ensure Company Personal Information remains protected, including encryption at-rest and support for encryption in-transit.
- Authorized individuals who access the network from external locations must utilize approved encryption and authentication methods and technology.
- Seagate does not permit the use of shared accounts to gain remote access to the network is not permitted.
- Seagate restricts remote access to access for required resources and services only.

Measures for the protection of Company Personal Information during storage:

- Lyve Services has implemented robust security measures to ensure Company Personal Information remains protected, including encryption at-rest and support for encryption in-transit.
- Seagate customer instances of the Lyve Cloud Services are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged.
- Measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer.

Measures for ensuring physical security of locations at which Company Personal Information are processed:

- Security measures for the Lyve Services are commensurate with the identified risk to information assets and services.
- Lyve Cloud Services incorporate physical and environmental security measures in facilities to minimize risk, avoid threats and eliminate vulnerabilities in order to protect information systems and personnel.
- Physical and environmental security is designed to prevent unauthorized physical access, damage and interference to Lyve Cloud Service's information assets and systems.
- Lyve Cloud Services protect secure areas with the establishment of entry controls to ensure only authorized personnel have access. The controls must include recording visitor access, restricting access where sensitive information is maintained to only authorized personnel, requiring users to wear a visible identification badge, and limiting individuals to only those physical areas needed to conduct business.
- Equipment, information, or software assets must not be taken off-site without authorization. The time limit for asset removal must be agreed upon by everyone involved and the return verified. Assets must be recorded as being moved off-site and the same record updated when the assets are returned.

Measures for ensuring events logging:

- Remote logging.
- An Information Security Management System Policy (ISMS) is in place.

Measures for ensuring system configuration, including default configuration: Measures to ensure that all in-scope systems and devices are compliant with baseline configuration settings.

- Seagate has in place a Change Management Policy.
- Seagate monitors changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of un-detected changes to production.
- Seagate has in place an Access Control Policy and Procedures.

Measures for internal Information Technology ("IT") and IT security governance and management:

- Seagate has an Information Security Management System (ISMS) in accordance with the ISO 27001:2013 standard.
- Seagate has in place a written information security policy, including supporting documentation.
- The authority and responsibility for managing Seagate's information security program has been delegated to the Chief Information Security Officer, who is authorized by senior management to take actions necessary to establish, implement, and manage Seagate's information security program.

Measures for certification/assurance of processes and products:

- Lyve Cloud Services has been audited by a third party and has achieved SOC 2 compliance, attesting to our commitment to controls that safeguard the confidentiality and privacy of information stored and processed in our service.
- Lyve Cloud Services is ISO 27001 certified, and its program includes, among other considerations: policies and procedures, asset management, access management, cryptography, physical and environmental security, business continuity policy, human resources security, disaster recovery, cloud and network infrastructure security, security compliance, third-party management, and security monitoring and incident response.

Measures for ensuring data minimization: Measures to reduce the amount of data collected.

- Company Personal Information collection is limited to the data that Company chooses to provide in the Lyve Services.
- Security measures are in place to provide only the minimum amount of access necessary to perform required functions.

Measures for ensuring data quality: Measures to ensure that the data pipeline creates and sustains good data quality.

- Seagate does not review or edit data, content or material created, stored, or made accessible through the Lyve Services including Company Personal Information, and Company has sole discretion on what data is put into the Lyve Services.
- Seagate has security controls to ensure data integrity.

Measures for ensuring limited data retention:

- Information owners must develop and implement procedures to ensure the proper disposal of information assets under their control.
- The Lyve Services protect information assets and arrange for their destruction when the asset has reached the end of its lifecycle as described in the record retention schedule. The secure destruction of these assets must ensure that no readable content remains intact.
- A secure automated process must be used for the destruction of electronic data and a secure manual process used for the destruction of hard copy records.
- After termination of all subscriptions associated with an environment, customer data submitted to the Lyve Cloud Services is retained in inactive status within the Lyve Cloud Services for 30 days, after which it is securely overwritten or deleted from production.
- After termination of all subscriptions associated with a Lyve Mobile Service, Company must use the cryptographic erase functionality on the device to securely erase Company's data from the device. When the Lyve Mobile Service device is returned to Seagate, authorized personnel execute an erasure of the device in a secure access-controlled location.

Measures for ensuring accountability: Businesses must maintain certain records of the personal data that they process.

- Privacy assessments are required when introducing any new product/service that involves processing personal data.
- Seagate assigns responsibility to ensure end-user privacy throughout the product lifecycle and through applicable business processes.

Measures for allowing Data portability and ensuring erasure:

- The Lyve Mobile Services are designed with portability in mind. Agreements address the secure transfer of business information between Lyve Cloud Services and external third parties.
- The Lyve Mobile Services establish and maintain documentation to protect information and physical media in transit so the information can be referenced in transfer agreements.

- The information security content of any agreement must reflect the sensitivity of the business information involved. Agreements may be electronic or manual and may be formal contracts.
- Company may be required to delete Company data off the services upon the expiration or earlier termination of the Agreement. When a customer chooses to intake or migrate their data into another Seagate service Seagate may, upon a successful intake or migration of such data, delete or otherwise dispose of any customer data stored in the original service.
- Lyve Services protect information assets and arrange for their destruction when the asset has reached the end of its lifecycle as described in the record retention schedule. The secure destruction of these assets must ensure that no readable content remains intact.
- Lyve Services use a secure automated process for the destruction of electronic data and a secure manual process used for the destruction of hard copy records.
- After termination of all subscriptions associated with the Lyve Services items of equipment containing storage media must be verified to ensure sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use. Storage media must be deleted or overwritten so the original data is non-retrievable.
- If Seagate decommissions or otherwise retires a hard drive that contains a copy of Company data then Seagate shall securely shred or destroy the drive rendering the data unreadable and destroyed in accordance with NIST 800-88, revision 1.

ANNEX C

LIST OF SUB-PROCESSORS

Sub-Processor	Purpose	Processing Location
Auth0 Inc.	Identity management.	USA and Germany

For agreements completed prior to October 14, 2021, please see the PDF attached here. Lyve Data Privacy Agreement prior to October 14, 2021