For agreements completed from June 20, 2024 to July 31, 2025

Data Privacy Agreement

EXHIBIT

This Data Privacy Agreement, including all annexes set out below (this "**DPA**"), is between the Seagate company named in the Agreement ("**Seagate**") and the supplier company named in the Agreement ("**Supplier**") (each a "**party**" and collectively the "**parties**").

Supplier has entered into one or more purchase orders, contracts and/or agreements, including statements of work (the "**Agreement(s)**)" with Seagate pursuant to which Supplier has agreed to provide certain services to Seagate as more particularly described in the Agreement(s) ("**Services**").

The parties are entering into this DPA to ensure that the Processing by Supplier of Personal Data provided to Supplier or collected by Supplier for Seagate and/or on its behalf, is done in a manner compliant with Data Protection Law(s) and its requirements regarding the collection, use and retention of Personal Data of data subjects.

This DPA is incorporated into and forms part of the Agreement(s). All capitalized words not defined in this DPA will have the meaning set forth in the Agreement(s). The parties acknowledge and agree as follows:

1. **DEFINITIONS**

    1. "**Affiliate**" means any entity which controls, is controlled by, or is under common control with the subject party.

    2. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully-diluted basis) then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

3. "**Data Privacy Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of Seagate Personal Information, or any other unauthorized Processing of Seagate Personal Information.

4. "**Data Protection Law(s)**" means all worldwide data protection, data security and privacy laws, rules, and regulations, applicable to Personal Data in question, including where applicable: (i) European Data Protection Law; (ii) all laws, rules and regulations of the United States, including US State Privacy Laws, as amended, superseded or updated from time to time; and (iii) applicable industry standards appropriate to the nature of the Personal Data.

5. "**European Data Protection Law(s)**" means all data protection laws and regulations applicable to the European Union ("**EU**") or the European Economic Area ("**EEA**"), including:

    1. the General Data Protection Regulation 2016/679 ("**EU GDPR**");

    2. 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**")

    3. the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances ("**Swiss DPA**"); and

    4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and

    5. applicable national implementations of (i), (ii), and (iii).

6. "**Data Subject**" is an identified or identifiable natural person about whom Personal Data may be Processed under this DPA

7. "**EU SCCs"** means 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.

8. "**Personal Data**" means any information which is protected as personal data, personal information or personally identifiable information or similarly defined terms under Data Protection Laws.

9. "**Processing**" or "**Process**" means, without limitation, operations performed on Seagate 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 Personal Data.

10. "**RestrictedTransfer**" means:

    1. where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission.

    2. where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject to or based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

    3. where Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not based on an adequacy decision recognized under Swiss data protection law.

11. "**Seagate Personal Information**" means any information that is protected as personal data, personally identifiable information or personal information under Data Protection Laws, which is created, owned, or provided by Seagate or for Seagate, that Supplier has access to, obtains, uses, maintains, or Processes on behalf of Seagate in connection with any Agreements between the parties and/or their Affiliates.

12. "**Sensitive Information**" means any of the following types of Seagate 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. For purposes of this DPA, Sensitive Information includes sensitive personal information, sensitive data, or similarly defined terms as defined under applicable Data Protection Laws, special categories of data as defined in the EU GDPR and the UK GDPR and sensitive personal data as defined in the Swiss DPA.

13. "**Standard Clauses**" means (as applicable) the EU SCCs, UK Addendum and Swiss modifications set out in Section 3.1(i)(3) of this DPA.

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

15. "**Supervisory Authority**" means any regulatory, supervisory, governmental, state agency, Attorney General or other competent authority with jurisdiction or oversight over compliance with the Data Protection Laws.

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

17. "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by Information Commissioners Office under

S.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

18. "**US State Privacy Laws"** means all applicable data privacy, data protection, and cybersecurity laws, rules, and regulations to which the Company Personal Data are subject.

19. The terms "**Controller**," "**Data Subject**," "**Processor**," "**Business**," "**BusinessPurpose**," "**CommercialPurpose**," "**Collect**," "**Consumer**," "**Share**," "**Sell**," "**SupervisoryAuthority**," and "**ServiceProvider**" shall have the meanings given to them under Data Protection Laws.

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

2. DATA SECURITY AND PROTECTION

1. **Status of the Parties.** In respect of Seagate Personal Information, the parties hereby acknowledge and agree that Supplier shall Process such Personal Data as a Processor, on behalf of Seagate. Supplier is hereby instructed to Process Personal Data to the extent necessary to provide the Services as set forth in the Agreement(s) and this DPA.

2. **CCPA Roles**. For the purposes of the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq ("**CCPA**") as amended by the California Privacy Rights Act ("**CPRA**") (where applicable), Supplier shall Process Personal Data as a Service Provider acting upon instructions of Seagate as a Business.

3. **Nondisclosure of Seagate Personal Information**. Supplier shall not disclose Seagate Personal Information in any manner for any purpose to any third party without obtaining prior written authorization from Seagate, other than disclosures to Sub-processors in accordance with Section2.5 below. Without limiting the foregoing, in no event may Supplier sell or otherwise disclose Seagate Personal Information to any third party for the commercial benefit of Supplier or any third party. Any person authorized to Process Seagate Personal Information must contractually

agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

4. **Limitations on Processing**. Supplier shall only Process Seagate Personal Information for the purposes of providing the Services to Seagate under the Agreement(s) and in accordance with Seagate's documented lawful instructions ("**Permitted Purposes**"). For these purposes, Seagate instructs Supplier to Process Seagate Personal Information for the purposes described in Annex I (Description of Transfer). Supplier shall not Process or permit the Processing of Seagate Personal Information except as necessary to provide services to Seagate in accordance with any Agreement between the parties and/or their Affiliates or other written instructions of Seagate.

5. **Processing Requirements**. Supplier shall at all times: (a) Process the Personal Data solely for the Permitted Purposes; and (b) not Process Personal Data for its own purposes or those of any third party. Supplier shall not: (i) Sell or Share Personal Data; (ii) retain, use or disclose Personal Data for any purposes other than for the Permitted Purpose(s), including retaining, using or disclosing Personal Data for a commercial purpose other than performing the Services under the Agreement(s); or (iii) retain, use or disclose Personal Data outside the direct business relationship between Seagate and Supplier. Supplier shall notify Seagate if it can no longer meet its obligations under CCPA/CPRA. Supplier certifies that it understands and will comply with the requirements and restrictions set out in this Section 2.5 and will further comply with the requirements applicable to Service Providers under the CCPA/CPRA. Further, the Parties acknowledge and agree that the exchange of Personal Data between the Parties does not constitute a Sale, nor form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement(s) or this DPA. In all cases, Supplier will not combine Personal Data received from Seagate with Personal Data that Supplier receives from, or on behalf of, another person or persons, or that Supplier Collects from any interaction between it and a Consumer. Both Seagate and Supplier represent that they have read and understand the requirements set forth under the CCPA/CPRA.

6. **Information Security Program**. Supplier will implement, maintain, monitor and, where necessary, update a comprehensive written information security program that contains appropriate administrative, technical, and physical safeguards to protect Seagate 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**"). The Information Security Program will include the requirements and measures listed in the Security Standards attached as Annex II.

7. **Restrictions on Sub-processors**. Supplier may disclose Seagate Personal Information to Sub-processors as necessary to perform its services for Seagate, subject to the conditions set forth in this Section 2.7. Supplier shall maintain a list of the Sub-processors to which it discloses Seagate Personal Information and will provide this list to Seagate upon Seagate's request. As of the effective date of the Agreement(s), if applicable, a current list of Supplier's Sub-processor(s) is included either in the Agreement(s) or in any other document provided by the Supplier to Seagate and signed by both parties, setting out the list of Sub-processor(s). Supplier shall notify Seagate at corporatecontracts@seagate.com at least **30 business days** before adding any Sub-processor to the list. If Seagate does not object to the proposed Sub-processor within **30 business days** of receipt of notice, the Sub-processor is deemed to have been approved. If Seagate objects to any Sub-processor having access to Seagate Personal Information, then Supplier shall not disclose Seagate Personal Information to the Sub-processor. If at any time either party finds a Sub-processor is not providing sufficient guarantees of security appropriate to the risk associated with the Seagate Personal Information being Processed, Seagate may in its sole discretion, remove the Sub-processor from the list. In the event a Sub-Processor is objected to or removed by Seagate, Supplier will be provided a reasonable amount of time to replace the Sub-processor. If Supplier cannot provide the Services without disclosing Seagate Personal Information to the objected to Sub-processor, then

Seagate may terminate any applicable Agreement(s) between the parties and/or their Affiliates without cost or liability owed to Supplier.

8. **Sub-processor Compliance and Breach**. Supplier's use of Sub-processors does not reduce Supplier's obligation to comply with this DPA or applicable Data Protection Laws. Supplier will be liable to Seagate for performance of the services, Data Privacy Breaches, and breaches of this DPA and applicable Data Protection Laws by its Sub-processors to the same extent as if Supplier breached.

9. **Obligations of Supplier Personnel and Sub-processors**. Supplier shall ensure that any person or Sub-processor who has access to Seagate Personal Information enters into a written agreement containing terms at least as restrictive as those in this DPA. Supplier shall ensure that all privacy and data protection obligations continue after their Processing for Seagate ends. This obligation continues in perpetuity, or alternatively, at least until Supplier has certified that all Seagate Personal Information has been deleted, destroyed, and is irretrievable.

10. **Limited Access**. Supplier shall limit access to Seagate Personal Information to Supplier Personnel or Sub-processors who require access for Supplier to perform its obligations under any Agreement(s) between the parties and/or their Affiliates or Seagate's written instruction, who have (a) been trained on data protection and security requirements, and (b) agreed to comply with data confidentiality requirements at least as restrictive as those required by Seagate during and after their Processing for Seagate.

11. **Notice of Requests or Complaints**. Unless prohibited by law, Supplier shall notify Seagate at data.protection.officer@seagate.com within 2 business days after receiving any request or complaint relating to the Processing of Seagate Personal Information, including:

    1. requests from a Data Subject for data portability, requests to access, change, delete, or restrict, and similar requests; or

    2. complaints or allegations that the Processing infringes on a Data Subject's rights.

12. **Supplier Responses**. Supplier shall not respond to any request or complaint under Section 2.11 unless expressly authorized to do so by Seagate. Supplier shall cooperate with Seagate with respect to any action taken relating to any request or complaint including, without limitation, deletion requests. Supplier shall seek to implement appropriate processes (including technical and organizational measures) to assist Seagate in responding to requests or complaints, unless prohibited by law.

13. **Requests for Disclosure.** Unless prohibited by law, Supplier shall immediately notify Seagate if Supplier receives any document requesting or purporting to compel the disclosure of Seagate 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; collectively, "**Disclosure Requests**"). If a Disclosure Request is not binding, Supplier will not respond. If a Disclosure Request is binding, Supplier shall, unless prohibited by applicable law, notify Seagate at least **48 hours** before responding so that Seagate may exercise such rights as it may have to prevent or limit the disclosure. Supplier shall exercise reasonable efforts to prevent and limit any disclosure and to preserve the confidentiality of Seagate Personal Information. Supplier shall cooperate with Seagate with respect to any action taken in response to Disclosure Request, including cooperating to obtain an appropriate protective order or other assurance to protect the confidentiality of the Seagate Personal Information.

14. **Cooperation.** Supplier shall assist Seagate in meeting its obligations under Data Protection Laws regarding (a) registration and notification; (b) accountability; (c) ensuring the security of Seagate Personal Information; and (d) fulfilling privacy and data protection impact assessments (including audits and risk assessments under Data Protection Laws) and related consultations of Supervisory Authorities.

15. **Participation in Regulatory Investigations**. Supplier shall assist and support Seagate in any investigation by any Supervisory Authority to the

extent the investigation relates to Seagate Personal Information Processed by Supplier or Supplier's Sub-processor.

16. **Notice of Potential Violations or Inability to Comply**. Supplier shall immediately notify Seagate if:

    1. Supplier has reason to believe that any instructions from Seagate regarding Processing of Seagate Personal Information would violate applicable law;

    2. Supplier has reason to believe that it is unable to comply with any of its obligations under this DPA or Data Protection Laws and it cannot cure this inability to comply within a reasonable timeframe; or

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

17. **Suspension or Adjustments for Compliance**. Seagate may suspend Supplier's or Sub-processors' Processing of Seagate Personal Information to prevent potential violations of or noncompliance with applicable law, this DPA, or any applicable Agreement(s) between the parties and/or their Affiliates related to privacy or data protection. Supplier shall cooperate with Seagate to adjust the Processing to remedy any potential violation or noncompliance. If adjustment is not possible, Seagate may terminate any applicable Agreement(s) between the parties and/or their Affiliates, without cost or liability owed to Supplier.

3. **DATA TRANSFERS**

1. **European Economic Area, United Kingdom, and Switzerland Standard Clauses.**

    i. The parties agree that where transfer of Seagate Personal Information from Seagate to Supplier is a Restricted Transfer, then it shall be subject to the appropriate Standard Clauses, which

are automatically incorporated by reference and form an integral part of this DPA as set out below:

1. in relation to Seagate Personal Information that is protected by EU GDPR, the EU SCCs will apply as follows:

    a. Seagate will be the data exporter and Supplier will be the data importer;

    b. Module Two (C2P) will apply;

    c. in Clause 7, the optional docking clause shall apply;

    d. in Clause 9 of Module Two (C2P), Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 7 of this DPA;

    e. in Clause 11, the optional language will not apply

    f. in Clause 17;

        i. for Module Two (C2P), Option 1 will apply, and

        ii. the EU SCCs will be governed by Irish law;

    g. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

    h. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and

    i. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

2. In relation to data that is protected by the UK GDPR, the EU SCCs:(i) shall apply as completed in accordance paragraph (1) above; and (ii) shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the parties and incorporated into and form an integral part

of this DPA. Any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex I and II of this DPA and table 4 in Part 1 shall be deemed completed by selecting neither party.

3. In relation to Seagate 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 DPA or the Agreement(s) contradicts, directly or indirectly, the Standard Clauses, the Standard Clauses shall prevail.

5. Supplier shall ensure that any Sub-processors also execute the Standard Clauses, where applicable.

ii. **Alternative Transfer Mechanisms:** To the extent that the Supplier adopts an alternative data export mechanism not described in this DPA (including any new version of or successor to the Standard Clauses adopted pursuant to applicable European Data Protection Law) for the transfer of Personal Data (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 (i) complies with European Data Protection Law, (ii) extends to the territories to which Personal Data is transferred, and (iii) satisfies the notification considerations below) and (iv) the Supplier executes such other and further documents and takes 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 Seagate Personal Information, Seagate acknowledges and agrees that subject to the notification considerations described below, the Supplier may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such Seagate Personal Information. The notification considerations require Supplier to notify Seagate at data.protection.officer@seagate.com at least 30 business days before implementing Alternative Transfer Mechanisms or any additional measures. If Seagate does not object to the proposed Alternative Transfer Mechanism or additional measures within 30 business days of receipt of notice, the Alternative Transfer

Mechanism or the measures are deemed to have been approved. If Seagate objects to any such Alternative Transfer Mechanism or additional measures, then Supplier shall not utilize such Alternative Transfer Mechanisms or any additional measures. In the event an Alternative Transfer Mechanism or additional measure is objected to by Seagate, then Seagate in its sole discretion, may terminate any applicable Agreement(s) between the parties and/or their Affiliates without cost or liability owed to Supplier.

iii. **Transfers out of countries with data export requirements.** If any Data Protection Laws require that further steps be taken in relation to any applicable data export restriction to permit the transfer of Seagate Personal Information to Supplier (including its Sub-processors), Supplier 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.

2. **Other Jurisdiction Provisions.** Where applicable, Supplier shall comply with the Requirements for Specific Jurisdictions, attached as Annex III.

4. COMPLIANCE AND ACCOUNTABILITY

1. **Compliance**. Supplier shall ensure that Supplier's and Sub-processors' Processing of Seagate Personal Information complies with all applicable laws, self-regulatory frameworks, and contract requirements applicable to Supplier and Sub-processor. Supplier shall annually review Supplier's and Sub-processors' practices to ensure they comply with this DPA and with all applicable laws. Supplier shall cooperate, at its own expense, with Seagate's requests that Supplier demonstrate compliance with the data protection and security terms referenced in this DPA.

2. **Records of Processing Activities.** Supplier will maintain an up-to-date record of the details of the Supplier's representative and data protection officer, categories of Processing activities performed, information

regarding cross-border data transfer, a general description of the security measures implemented in respect of the Processed data, the name, contact and Processing details of each Sub-processor of Seagate Personal Information, and, where applicable, any Sub-processors' representative and data protection officer. Upon request, Supplier will provide an historical and current copy of this record to Seagate or Supervisory Authority upon request.

3. **Audit**. Supplier shall make available to Seagate, on written request, all information necessary to demonstrate compliance with this DPA and Data Protection Laws, and shall allow for and contribute to audits, including onsite inspections, by Seagate or an independent third-party audit or mandated by Seagate in relation to the Processing of Seagate Personal Information. Any such independent third-party auditor shall be required to enter into a non-disclosure agreement with the parties. Supplier shall remedy any non-compliance within a reasonable amount of time. If remediation is not possible, Seagate may terminate any applicable Agreement(s) between the parties and/or their Affiliates, without cost or liability owed to Supplier.

5. SUPPLIER RESPONSIBILITIES AFTER A DATA PRIVACY BREACH

1. **Notification of Data Privacy Breach**. Supplier shall notify Seagate in writing of a known or suspected Data Privacy Breach immediately, and in any event within **24hours** after first learning of the potential Data Privacy Breach, and shall immediately:

    1. notify Seagate at data.protection.officer@seagate.com of the Data Privacy Breach;

    2. investigate or provide required assistance in the investigation of the Data Privacy Breach;

    3. provide Seagate with detailed information about the Data Privacy Breach, including but not limited to the categories, location, and approximate number of Data Subjects concerned and the categories, location, and approximate number of Seagate Personal Information records, and continue to provide Seagate

promptly with additional information about the Data Privacy Breach as it becomes available;

4. take all commercially reasonable steps to mitigate the effects of the Data Privacy Breach, or assist Seagate in doing so; and

5. implement a remediation plan, subject to Seagate's approval, and monitor the resolution of Data Privacy Breaches and vulnerabilities related to Seagate Personal Information to ensure that appropriate corrective action is taken on a timely basis.

2. **Containment and Remedy**. Supplier shall immediately contain and remedy any Data Privacy Breach and prevent any further Data Privacy Breach; and Supplier shall take all actions necessary to comply with applicable Data Protection Laws and industry standards to contain and remedy the Data Privacy Breach.

3. **Communications**. Supplier 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, Seagate, without Seagate's prior approval.

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

5. **Cooperation.** Supplier shall cooperate with Seagate in any litigation, investigation, or other action Seagate requires to protect Seagate's rights relating to the use, disclosure, protection, and maintenance of Seagate Personal Information. Supplier further agrees to provide reasonable assistance and cooperation requested by Seagate and/or Seagate's designated representatives, in the furtherance of any correction, remediation, or investigation of any Data Privacy Breach and/or the mitigation of any potential damage, including any notification that Seagate may determine appropriate to send to affected Data Subjects, regulators or third parties, and/or the provision of any credit reporting service that Seagate deems appropriate to provide to affected Data

Subjects. Supplier will be responsible for Seagate's reasonable expenses related to a Supplier Data Privacy Breach, including but not limited to investigation, remediation, and notification.

6. RETURN AND SECURE DELETION OF SEAGATE PERSONAL INFORMATION

1. **Data Integrity**. Supplier shall comply with all Seagate instructions to maintain data integrity, including (a) disposing of Seagate Personal Information that is maintained by Supplier but that is no longer necessary to provide Services, unless the retention of Seagate Personal information is required by Data Protection Laws; (b) ensuring that any Seagate Personal Information created by Supplier on Seagate's behalf is accurate and kept up to date; and (c) upon Seagate's request, allow Seagate to access any Seagate Personal Information, all in accordance with applicable laws.

2. **Return and Deletion of Seagate Personal Information.** Upon the earlier of (a) request by Seagate or (b) the expiration or earlier termination of the Agreement(s) between the parties and/or their Affiliates related to the Processing of Seagate Personal Information, at Seagate's direction, Supplier shall, and shall direct its Sub-processors to, export the Seagate Personal Information or provide Seagate, or its third party designee, with the ability to export all Seagate Personal Information in a machine readable and interoperable format determined by Seagate, unless the retention of Seagate Personal information is required by Data Protection Laws. Supplier shall maintain the Seagate Personal Information for as long as Seagate determines is reasonably necessary to allow Seagate to fully access and export the Seagate Personal Information, at no cost to Seagate. Each party shall identify a contact person to migrate the Seagate Personal Information and shall work promptly, diligently, and in good faith to facilitate a timely transfer. Within **90 days** after Seagate (a) confirms that Seagate Personal Information was received and migrated correctly, or (b) informs Supplier of its election to not migrate the Seagate Personal Information, Supplier and Sub-processors shall securely destroy all Seagate Personal Information, delink Seagate's workspace identifiers, and overwrite with new data or otherwise destroy

the Seagate Personal Information through an approved sanitization method.

3. **Destruction of Seagate Personal Information**. If Supplier disposes of any paper, electronic or other record containing Seagate Personal Information, Supplier will do so by taking all reasonable steps (based on the sensitivity of the Seagate Personal Information) to destroy Seagate Personal Information, unless the retention of Seagate Personal information is required by Data Protection Laws by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying the Seagate Personal Information in such records to make it unreadable, unreconstructable and indecipherable. If Supplier decommissions or otherwise retires a hard drive that contains a copy of Seagate Personal Information then Supplier shall securely shred or destroy the drive rendering the Seagate Personal Information unreadable and destroyed in accordance with NIST 800-88, revision 1. Supplier shall certify in writing that the drive has been shredded or destroyed and that that the Seagate Personal Information cannot be read, retrieved, or otherwise reconstructed.

4. **Notice of Any Retention**. If Supplier has a legal obligation to retain Seagate Personal Information beyond the period otherwise permitted by this DPA, Supplier shall notify Seagate in writing of its obligation, shall not further Process the Seagate Personal Information beyond retaining such information to fulfill Supplier's legal obligation, and shall return or destroy the Seagate Personal Information as soon as possible after the legally required retention period ends. This DPA will remain in effect until Supplier has ceased to have custody or control of or access to any Seagate Personal Information.

5. **Documentation.** Supplier shall document its retention and disposal of Seagate Personal Information pursuant to this DPA. Upon Seagate's request, Supplier shall provide documentation of retention and a written certification that Seagate Personal Information has been securely destroyed in accordance with this DPA.

7. **MISCELLANEOUS**

1. **Term**. This DPA will remain in effect until (i) there is no other active Agreement(s) between the parties and (ii) Supplier has ceased to have custody or control of or access to any Seagate Personal Information. Supplier will Process Seagate Personal Information until the relationship terminates as specified in the Agreement. Supplier's obligations and Seagate's rights under this DPA will continue in effect so long as Supplier Processes Seagate Personal Information.

2. **Order of Precedence.** In case of discrepancies between this DPA and any Agreement(s) between the parties and/or their Affiliates, the provisions of this DPA will prevail except for any discrepancies involving Annex II (Security Standards), in which case the other Agreement(s) will prevail, to the extent that the security standards in the other Agreement(s) are in addition to the minimum requirements set out in Annex II. This DPA shall not limit or restrict but shall only be deemed to supplement the Standard Clauses.

3. **Updates.** Supplier will reasonably cooperate to update this DPA as needed to ensure compliance with applicable laws and regulations.

4. **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 were 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 Supplier.

5. **Disclosure of DPA to Supervisory Authority**. Seagate may provide a summary or a copy of this DPA to any Supervisory Authority.

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

ANNEX I
DATA PROCESSING DESCRIPTION

This Annex I forms part of the Standard Clauses.

MODULE TWO: Transfer – Controller to Processor (relevant for Seagate Personal Information) (C2P)

A. LIST OF PARTIES

DATA EXPORTER	
Name and address	Seagate Technology LLC signing on behalf of Affiliates and subsidiaries 47488 Kato Road, Fremont, CA, 94538
Contact Person's Name and Contact Details	Seagate Technology LLC signing on behalf of Affiliates and subsidiaries 47488 Kato Road, Fremont, CA, 94538 data.protection.officer@seagate.com
Activities relevant to the data transferred under these Standard Clauses	Seagate Technology LLC, signing on behalf of Affiliates and subsidiaries, is a provider of hardware products and software solutions and services to support business processes of various industry segments.
Signature and date:	By entering into the Agreement(s) which incorporates this DPA, data exporter is deemed to have signed these Standard Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement(s).
Data exporter Role (Controller/Processor):	Set forth in Section 2.1 (Status of the Parties) of this DPA.

DATA IMPORTER	
Name and address	Supplier name and address (as specified in the Agreement(s)

Contact Person's Name, Position and Contact Details:	Supplier name and address (as specified in the Agreement(s)
Activities relevant to the data transferred under these Standard Clauses:	Supplier is a service provider providing services and support to data exporter, as described in the Agreement(s).
Signature and date:	By entering into the Agreement(s) which incorporates this DPA, data importer is deemed to have signed these Standard Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement(s).
Data importer role	Set forth in section 2.1 (Status of the Parties) of this DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects	The personal data transferred may concern the following categories of data subjects: - past and present: o employees, advisors, consultants, suppliers, contractors, subcontractors, and agents of Seagate; o business partners and potential business partners of Seagate, and their employees, partners, advisors, consultants, suppliers, contractors, subcontractors, and agents; o potential marketing leads and past and present consumers; o past and present customers of Seagate, and their employees, partners, advisors, consultants, suppliers, contractors, subcontractors, and agents.

Categories of personal data transferred	Personal data provided by Seagate or on behalf of Seagate to Supplier, or collected by the Supplier, that relates to the Categories of data subjects set out above, as necessary for Supplier to provide the Services to Seagate under the Agreement(s) and in accordance with Seagate's documented lawful instructions, which may include contact information, such as first name, last name, email address, business address, phone number and any other personal data provided by Seagate.
Sensitive Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved**	As set out in the Agreement(s)
Frequency of the transfer	Continuous, unless otherwise set out in the Agreement(s) or in a document between the parties.
Nature of the Processing/Processing Activities	As described in the Agreement(s).
Purpose of the data transfer and processing	To provide the Services under the relevant Agreement(s).
Period for which the personal data will be retained, or, if not possible, the criteria	The personal data will be retained: (a) in accordance with Section 6.2 of this DPA (Return and Deletion of Seagate Personal Information); or (b) as otherwise required by law; or

used to determine that period	(c) or for the duration set out in the Agreement(s) or another document between the parties that contains the relevant information applicable to the relevant Services; whichever is the longer.
If transferring to sub-processors, also specify subject matter, nature and duration of the processing	Supplier shall provide the subject matter, nature and duration of processing for transfers to sub-processors to data.protection.officer@seagate.comif this information is not otherwise already set out in the Agreement(s) or an additional document agreed between the parties.

C. COMPETENT SUPERVISORY AUTHORITY

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 EU 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 Personal 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 II
SECURITY STANDARDS

This Annex II forms part of the Standard Clauses.

This Annex II represents the **minimum-security measures** that will be taken by Supplier. If any agreement(s) between the parties requires Supplier to have a higher level or more extensive security measures, Supplier will abide by those terms. Supplier must maintain and enforce various policies, standards and processes

designed to secure Seagate Personal Information and other data per industry standards, for example NIST Cyber Security Framework and ISO 27001 or 27002, to which Supplier employees are provided access.

1. **Information Security Policies and Standards.** Supplier must implement security requirements for staff and all subcontractors, suppliers, or agents who have access to Seagate Personal Information that are designed to:

    a. prevent unauthorized persons from gaining access to Seagate Personal Information processing systems (physical access control);

    b. prevent Seagate Personal Information processing systems being used without authorization (logical access control);

    c. ensure that persons entitled to use a Seagate Personal Information processing system can only gain access to such Seagate Personal Information as they are entitled to access in accordance with their approved access rights and that, in the course of processing or use and after storage Seagate Personal Information cannot be read, copied, modified or deleted without authorization (data access control);

    d. ensure that Seagate Personal Information cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage, and that the target entities for any transfer of Seagate Personal Information by means of data transmission facilities can be established and verified (data transfer control);

    e. ensure the establishment of an audit trail to document whether and by whom Seagate Personal Information have been entered into, modified in, transferred, or removed from Seagate Personal Information processing (entry control);

    f. ensure that Seagate Personal Information is Processed solely in accordance with the instructions (control of instructions);

    g. ensure that Seagate Personal Information is protected against accidental destruction or loss (availability control); and

h. ensure that Seagate Personal Information collected for different purposes can be Processed separately (separation control).

Supplier will conduct periodic risk assessments and reviews, and, as appropriate, revise its information security practices at least annually or whenever there is a material change in Supplier's business practices that may reasonably affect the security, confidentiality or integrity of Seagate Personal Information, provided that Supplier will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of Seagate Personal Information.

2. **Physical Security.** Supplier must maintain commercially reasonable security systems at all Supplier sites at which an information system that uses or houses Seagate Personal Information is located. Supplier reasonably restricts access to such Seagate Personal Information appropriately.

3. **Organizational Security.**

1. When media are to be disposed of or reused, procedures must be implemented to prevent any subsequent retrieval of any Seagate Personal Information stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures must be implemented to prevent undue retrieval of Seagate Personal Information stored on them.

    2. Supplier must implement security policies and procedures to classify Sensitive Information assets, clarify security responsibilities and promote awareness for employees.

    3. All Seagate Personal Information security incidents must be managed in accordance with appropriate incident response procedures.

    4. Supplier must encrypt, using industry-standard encryption tools, all Sensitive Information in transit and at rest.

4. **Network Security.** Supplier must maintain network security using commercially available equipment and industry-standard techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.

5. **Access Control.** Supplier must maintain appropriate access controls, including, but not limited to, restricting access to Seagate Personal Information to the minimum number of Supplier Personnel who require such access.

    1. Only authorized staff may grant, modify, or revoke access to an information system that uses or houses Seagate Personal Information. Supplier must maintain proper access records, which will be presented to Seagate upon Seagate's request.

    2. User administration procedures must define user roles and their privileges and how access is granted, changed, and terminated; address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms.

    3. All employees of Supplier must be assigned unique user-IDs.

    4. Access rights must be implemented adhering to the "least privilege" approach.

    5. Supplier must implement commercially reasonable physical and electronic security to create and protect passwords.

6. **Virus and Malware Controls.** Supplier must install and maintain the latest anti-virus and malware protection software on the system and have in place scheduled malware monitoring and system scanning to protect Seagate Personal Information from anticipated threats or hazards and protect against unauthorized access to or use of Seagate Personal Information.

7. **Personnel**. Prior to providing access to Seagate Personal Information to Supplier Personnel, Supplier must require Supplier Personnel to comply with Supplier's information security program. Supplier must implement a security awareness program to train personnel about their security obligations. This program will include training about data classification obligations; physical security controls; security practices; and security incident reporting. Supplier will have clearly defined roles and responsibilities for the employees. Screening will be implemented before employment with terms and conditions of employment applied appropriately. Supplier employees must strictly follow established security policies and procedures. A disciplinary process must be applied if employees commit a Data Privacy Breach.

8. **Business Continuity**. Supplier implements appropriate back-up and disaster recovery and business resumption plans. Supplier reviews both business continuity plan and risk assessment regularly. Business continuity plans are being tested and updated regularly to ensure that they are up to date and effective.

9. **Primary Security Manager**. Supplier must notify Seagate of its designated primary security manager. The security manager will be responsible for managing and coordinating the performance of Supplier's obligations set forth in Supplier's information security program and in this DPA

10. **Audit**. Seagate reserves the right to audit Supplier commitments as stated in this Annex II, in accordance with section 4.4 "Audit" of this DPA.

11. **Breach**. If it is determined Supplier is in breach of this DPA, Supplier must remediate any such breach without undue delay and in any event within **30 calendar days**. Any known or suspected Data Privacy Breach shall be governed by section 5. "Supplier Responsibilities After a Data Privacy Breach" of this DPA.

Annex III
DATA PRIVACY REQUIREMENTS FOR SPECIFIC JURISDICTIONS

The following requirements apply to the jurisdictions specified:

1. **AUSTRALIA**

    1. **Applicability**. The provisions of this Section 1 apply where (a) Supplier receives or accesses Seagate Personal Information from a Seagate Affiliate located in Australia; or (b) Seagate notifies Supplier that Seagate Personal Information is subject to these requirements.

    2. **Membership of a Professional or Trade Association**. The term "Sensitive Information" also includes Personal Information about an individual's membership of a professional or trade association.

    3. **Australian Privacy Principles**. The Supplier must comply with any applicable obligations under the Privacy Act 1988 (Cth), including the

Australian Privacy Principles, when dealing with Seagate Personal Information or otherwise providing the services pursuant to this DPA.

4. **Notice of use or disclosure for enforcement purposes**. If Supplier uses or discloses Personal Information for one or more enforcement activities conducted by, or on behalf of, an enforcement body, Supplier shall keep a written record of the use and disclosure and promptly provide a copy of the record to Seagate, unless prohibited by law.

5. **Australian government related identifiers.** Where the Personal Information includes Australian government related identifiers Supplier (a) shall not adopt the Australian government related identifier for an individual as its own identifier of the individual unless expressly directed to do so by Seagate; and (b) shall not use or disclose the Australian government related identifier except where reasonably necessary to verify the identity of the individual, or otherwise where directed to do so by Seagate.

6. **Collection of Personal Information**. Where Seagate's instructions to Supplier require Supplier to collect personal information on Seagate's behalf, Supplier must (a) seek instructions from Seagate regarding (i) any information that must be provided to the Data Subject in connection with the collection of the Data Subject's personal information; and (ii) any opt-in consents required for direct marketing purposes; and (b) not collect any Sensitive Information or without the Data Subject's consent.

7. **Supplier Agreements with the Australian Government**. If Seagate is a contracted service provider to an Australian government entity at federal, state or territory level, and to the extent Seagate is bound to comply with additional data protection obligations by virtue of an agreement with the relevant government entity, Seagate will impose equivalent obligations upon Supplier, as required under applicable Australian law. Seagate and Supplier agree to enter into additional agreements, if needed, to reflect those obligations.

2. **CHINA**

1. **Applicability**. The provisions of this Section 2 apply where Supplier receives or accesses Seagate Personal Information from a Seagate Affiliate located in China, or (b) Seagate notifies Supplier that Seagate Personal Information is subject to these requirements.

2. **PIPL Roles**. Under the Personal Information Protection Law of PRC (PIPL), Seagate will act the role of Personal Information Processor, who will decide the purposes and manners of Processing. Supplier will be the Entrust Party who Process Personal Information on behalf of Seagate according to the requirements of this DPA and Seagate instructions.

3. **Sub-Processors.** Notwithstanding Section 2.4 of the DPA, Supplier will not engage any Sub-processor to Process Seagate Personal Information without Seagate's express consent. The terms of such consent are subject to the DPA's Section 2.5.

4. **Limited Processing Time**. Supplier shall Process the Seagate Personal Information only for the period of time necessary to achieve the purposes of Processing unless the parties have agreed on a different duration.

5. **Restricted transfers**. Supplier shall not transfer Seagate Personal Information outside of China without Seagate's express consent if the Seagate Personal Information is stored or held in China. Seagate hereby provides consent for Supplier to transfer such Seagate Personal Information where necessary, provided Supplier has taken all measures to comply with the Data Protection Laws for the protection of such Seagate Personal Information

3. **INDIA**

1. **Applicability**. The provisions of this Section 3 apply where the Information Technology Act, 2000 ("**IT Act**") and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules") as amended and superseded from time to time applies to Supplier's Processing Of Seagate Personal Information provided by a Seagate Affiliate in India, regardless of whether the Processing takes place in India

2. Clause 1.12 of the DPA shall be modified to include the categories of personal data specified in Section 3 of the Privacy Rules

4. **JAPAN**

1. **Applicability**. The provisions of this Section 3 apply to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in Japan.

2. **Supplier Personnel**. Supplier will be responsible for supervising its Supplier Personnel in their compliance with the DPA.

3. **Employment Management Measures**. Supplier shall protect Seagate Personal Information relating to employment management as provided by Ministry of Health, Labor, and Welfare ("MHLW") Employment Management Guidelines.

4. **Personal Information Learned Through Employment**. Supplier shall ensure that its employees do not divulge or misappropriate the Seagate Personal Information learned through their employment.

5. **Consent before Transfer or Disclosure**. Supplier shall obtain prior written consent from Seagate before disclosing or transferring social security and tax numbers to any third party (including any Affiliate) that is not a party to the DPA, including any Sub-processors.

6. **Return or Destroy after Purpose Achieved**. Supplier shall stop Processing and return or destroy Seagate Personal Information in its possession when it has achieved the purpose for which it was collected.

7. **Backup Purposes**. Supplier shall not copy or reproduce Seagate Personal Information except for backup purposes.

5. **SOUTH KOREA**

1. **Applicability**. The provisions of this Section 4 apply to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in South Korea.

2. **Limited Access**. Supplier shall limit access to Personal Information to Supplier Personnel who reasonably require such access for the purposes of the Processing.

3. **Required Safeguards**. Supplier shall establish and maintain safeguards including:

    1. internal procedures for secure handling of Personal Information;

    2. technical safeguards such as firewalls, anti-virus, and anti-malware software;

    3. physical access restrictions, such as locks;

    4. measures to prevent alteration or falsification of access logs or records of Processing;

    5. measures to securely store and transmit Personal Information, such as encryption of Personal Information where required by the Personal Information Protection Act (PIPA), the Enforcement Regulations of PIPA, the Act on Promotion of Information and Communications Network Utilization and Protection of Information (PICNU), the Enforcement Regulations of PICNU ("PICNU Regulations"), the Utilization and Protection of Credit Information Act (UPCIA) or other Korean law, as applicable.

4. **Encryption of Peculiar Identification Data.** Supplier shall encrypt resident registration numbers, driver's license numbers, and passport numbers when:

    1. transmitted through an information or communications network;

    2. stored on portable storage media or peripherals;

    3. stored on any external computer network, or in a demilitarized zone, or on any personal computer or mobile device; or

    4. stored on Supplier's internal network if Supplier's systems fail to meet Seagate-specified risk criteria.

5. **Encryption of Password and Biometric Data.** Supplier shall encrypt all passwords and biometric data stored in any form.

6. **Information before Disclosure.** Before disclosing or transferring Seagate Personal Information to a third-party data processor, Supplier shall inform Seagate reasonably in advance. Upon Seagate's request, Supplier will provide the following information: (a) the Processing activities to be subcontracted; (b) the identity of the third-party data processor; and (c) any changes to (a) or (b).

7. **Training**. Supplier will participate in any training that Seagate may elect to provide to Supplier to safeguard against Seagate Personal Information being stolen, leaked, altered, or damaged during the course of Processing such Seagate Personal Information.

6. SINGAPORE

1. **Applicability**. The provisions of the Section 6 apply where the Singapore Personal Data Protection Act 2012 (No. 26 of 2012) applies to Supplier's Processing of Seagate Personal Information.

2. Clause 1.3 of the DPA shall be replaced with the following:

   1.3 "Data Privacy Breach" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of Seagate Personal Information, including: (a) the unauthorized access, collection, use, disclosure, copying, modification or disposal of Seagate Personal Information; or (b) the loss of any storage medium or device on which Seagate Personal Information is stored in circumstances where the unauthorized access, collection, use, disclosure, copying, modification or disposal of the Seagate Personal Information is likely to occur.

3. Clause 5.1 of the DPA shall be replaced with the following:

   5.1 Notification of Data Privacy Breach. Where Supplier has reason to believe that a Data Privacy Breach has occurred, Supplier shall notify Seagate in writing of the Data Privacy Breach without undue delay, and shall:

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

b. provide Seagate 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 Seagate in doing so at Supplier's expense.

7. **TAIWAN**

1. **Applicability**. The provisions of this Section 5 apply to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in Taiwan.

2. **Sub-Processors**. Notwithstanding Section 2.4 of the DPA, Supplier will not disclose or transfer Seagate Personal Information to or allow access to Seagate Personal Information to any Sub-processor without Seagate's express written consent.

3. **Limited Processing Time**. Supplier shall Process the Seagate Personal Information only for the period of time necessary to achieve the purposes of Processing, unless the parties have agreed on a different duration.

4. **Preserve Access Records**. Supplier shall preserve access records for as long as necessary to ensure they are periodically reviewed for instances of unauthorized access.

8. **THAILAND**

1. **Applicability**. The provisions of this Section 6 apply where the Thailand's Personal Data Protection Act, B.E. 2562 (2019) ("PDPA") as amended and superseded from time to time applies to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in Thailand.

2. Clause 1.3 of the DPA shall be replaced with the following:

   1.3 "Data Privacy Breach" means a breach of security measures which causes loss, access, use, modification, or disclosure of personal data unlawfully or without authorization, resulting from an intentional, willful, negligent, accidental, unauthorized or unlawful act, or an act related to computer crimes, cyber threats, mistakes or accidents, or any other act, as prescribed by the notification issued under the PDPA.

3. Clause 1.12 of the DPA shall be modified to include the categories of personal data specified in Section 26 of the PDPA

4. **Security Standards**. Supplier shall exercise its best efforts and take all reasonable actions to implement and maintain security standards shall at a minimum, be in accordance with the requirements in Annex II and with the provisions and requirements stipulated under the PDPA and any other rules, regulations, notifications and/or orders issued by the virtue thereof, including without limitation, the Notification of the Personal Data Protection Committee re: Security Measures of the Data Controller B.E. 2565 (2022), as may be amended, supplemented or replaced from time to time.

The Data Privacy Agreement is effective from June 20, 2024, onward.
For agreements completed from December 8, 2022 to June 20, 2024, please see the PDF here.Data Privacy Agreement June 20, 2024
For agreements completed from August, 11, 2020 to December 8, 2022, please see the PDF here.Data Privacy Agreement December 8, 2022
For agreements completed from November 20, 2019, to August 10, 2020, please see the PDF here.Data Privacy Agreement August 10, 2020
For agreements completed from March 31, 2019, to November 19, 2019, please see the PDF here.Data Protection Requirements November 20, 2019
For agreements completed prior to March 31, 2019, please see the PDF here.Data Protection Requirements March 31, 2019