COHESITY, INC.
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("***DPA***", including its Schedules and Appendices) is subject to and forms part of the End User License Agreement, Terms of Service, Evaluation Agreement or other written agreement between Cohesity, Inc. ("***Cohesity***") and Cohesity's customer ("***Customer***") for Cohesity's provision of the data storage products and/or services specified in Schedule 3 (the "***Services***") (collectively the "***Agreement***"). This DPA is effective on the same date as the Agreement unless this DPA is separately executed in which case it is effective on the date of last signature (the "***Effective Date***").

1. DEFINITIONS

Capitalized terms used in this DPA shall have the following meanings:

1.1 ***"Adopting Country"*** has the meaning given in Section 10.2 of this DPA.

1.2 "***Affiliate***" means, with respect to a party, any individual, company, or other entity, directly or indirectly, Controlled by, or under common Control with, such Party, but, for clarity, excluding those individuals, companies or entities that are Controlling such Party. "***Control***" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.3 ***"Authorized Affiliate"*** means any of Customer's Affiliate(s) who (a) is subject to the Data Protection Laws and Regulations, and (b) is permitted to use or gain the benefit of the Services pursuant to the Agreement between Customer and Cohesity, whether or not it entered its own order for Cohesity Products or Services ("**Order**") or is a 'Customer' or equivalent as defined under the Agreement.

1.4 "***Controller***" means the entity which determines the purposes and means of the Processing of Personal Data.

1.5 "***Customer Data***" means any data, files, text, images, graphics, software, or other materials and information Customer, its employees, contractors, agents or users ("***Users***") uploads to, transfers to, or otherwise transmits or sends to Cohesity including through Cohesity's customer support portal(s), but excludes for avoidance of doubt information stored or otherwise Processed in or through Cohesity hardware products and equipment ("***Hardware***") or a SaaS Offering to the extent Cohesity does not access or Process same.

1.6 "***Data Protection Laws and Regulations***" means laws and regulations regarding privacy and data protection, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, the California Consumer Privacy Act (CCPA), and the Personal Information Protection and Electronic Documents Act (Canada) in each case as and to the extent applicable to Cohesity as a matter of law with respect to the Processing of Personal Data hereunder.

1.7 "***Data Subject***" means the identified or identifiable person to whom Personal Data relates.

1.8 "***GDPR***" means Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data.

1.9 ***"GDPR SCCs"*** means Standard Contractual Clauses between Cohesity and Customer and attached hereto as Schedule 2, Part 1 pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021.

1.10 "***Personal Data***" means any information defined as "personal data", "personal information" or "personally identifiable information" under applicable Data Protection Laws and Regulations and which (i) relates to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person and (ii) is Customer Data.

1.11 "***Processing***" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12 "***Processor***" means the entity which Processes Personal Data on behalf of the Controller.

1.13 "***SCCs***" means model contract language applicable to Cohesity and Services, dictated by a particular jurisdiction and determined to provide a sufficient legal basis for cross-border transfers by a competent authority with jurisdiction over Cohesity as set out in Schedule 1 of this DPA, including GDPR SCCs and UK SCCs.

1.14 "***Sub-Processor***" means any Processor engaged by Cohesity, which may include a Cohesity Affiliate.

1.15 "***Supervisory Authority***" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

1.16 ***"United Kingdom Standard Contractual Clauses ("UK SCCs")"*** means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, with the option of the Alternative Part 2 Mandatory Clauses attached hereto as Schedule 1, Part 2 of this DPA.

Capitalized terms used but not defined herein shall have their meaning given in the Agreement.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. The parties acknowledge and agree that, with regard to the Processing of Personal Data, Customer is the Controller, Cohesity is the Processor, and if Cohesity engages Sub-Processors it will be pursuant to Section 5 below.

2.2 **Customer's Processing of Personal Data and Compliance with Law**. Customer shall, in its use of the Services, Process Personal Data (and information relating to identified or identifiable persons provided by Cohesity or its employees) in accordance with the requirements of Data Protection Laws and Regulations. Customer's instructions to Cohesity for the Processing of Personal Data shall also comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for (i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, (ii) ensuring appropriate security measures are applied to the Personal Data before and during Processing, including without limitation (a) properly implementing SSL or other encryption appropriate to the nature of content being transmitted, (b) obtaining lawful valid consent from or providing notification to Data Subjects for Processing in accordance with applicable Data Protection Laws and Regulations (including but not limited to explicit notification of and consent to Processing and storage out of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom as contemplated by the Agreement). Customer is responsible for complying with any requirements to notify Data Subjects of Processing hereunder.

2.3 **Cohesity's Processing of Personal Data**. Cohesity shall Process any Personal Data subject to the Data Protection Laws and Regulations in accordance with such Data Protection Laws and Regulations as applicable to Cohesity in its provision of the Services. Cohesity shall treat Personal Data that is Confidential Information in its possession as confidential and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with and as reasonably contemplated by the Agreement; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email or through any support portal) where such instructions are consistent with the terms of the Agreement and Data Protection Laws and Regulations. For clarity, Cohesity shall not be deemed to Process information or data Customer inputs into Products or Services except to the extent same is provided by Customer to Cohesity and accessed or Processed by Cohesity, e.g. in connection with support and maintenance services, or in certain SaaS Offerings. In addition, Cohesity shall not be responsible for, and this DPA does not cover, environments in which Cohesity Products or Services are hosted which are not under Cohesity's control. Entry into the Agreement shall be deemed Customer's express instructions to Cohesity to Process Personal Data as reasonably contemplated by the Agreement, including Processing initiated by Users in their use of the Services and Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) consistent with the Agreement.

2.4 **Details of the Processing**. The subject-matter of Processing of Personal Data by Cohesity is the performance of the Services pursuant to the Agreement, which may include, as applicable, the provision of support services under a support contract and Cohesity's use of Personal Data in connection with the sale to Customer of Hardware. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA. Notwithstanding anything else, Cohesity may modify the data Processing terms applicable to Services by posting an updated version of this DPA on www.cohesity.com/agreements.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests**. Cohesity shall, to the extent legally permitted, promptly notify Customer if Cohesity receives a request from a Data Subject to exercise the Data Subject's right of access, right to

rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, its right not to be subject to an automated individual decision making or other 'subject access' right under applicable law ("***Data Subject Request***"). Taking into account the nature of the Processing, Cohesity shall assist Customer by appropriate technical and organizational measures, insofar as this is possible and commercially practicable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Cohesity shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Cohesity is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Cohesity's provision of such assistance.

4. COHESITY PERSONNEL

Cohesity shall use commercially reasonable efforts to ensure that:

4.1 its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Cohesity shall ensure that such confidentiality obligations survive the termination of the personnel engagement to the extent permitted by law for a reasonable period.

4.2 the reliability of any Cohesity personnel engaged in the Processing of Personal Data.Cohesity's access to Personal Data is limited to those personnel with a need to know in rendering the Services in accordance with the Agreement.

4.3 Any questions or concerns with respect to this DPA and/or data security and privacy may be directed to privacy@cohesity.com.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-Processors**. Customer acknowledges and agrees that Cohesity may engage third-party Sub-Processors in connection with the provision of the Services. Cohesity shall enter into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-Processor.

5.2 **List of Current Sub-Processors and Notification of New Sub-Processors**. Cohesity shall make available to Customer the then current list of Sub-Processors for the Services at www.cohesity.com/agreements/ or by other means, and such list shall be deemed the "agreed list" referred to in Clause 9 of the GDPR SCCs ("***Sub-Processor Lists***"). Customer may request email notification of updates to the Sub-Processor Lists by emailing privacy@cohesity.com and providing the email address to which such notifications should be sent, together with other reasonable information Cohesity may request. Notifications pursuant to Clause 9 of the GDPR SCCs are subject to best efforts and, where circumstances require for operational reasons, may be on shorter notice.

5.3 **Objection Right for New Sub-Processors**. Customer may object to Cohesity's use of a new Sub-Processor by notifying Cohesity promptly in writing within ten (10) business days after an updated Sub-Processor List is made available in accordance with Section 5.2. In the event Customer objects to a new Sub-Processor on reasonable grounds, Cohesity will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening the Customer. If Cohesity is unable to make available such change within a reasonable period of time (which shall not exceed thirty (30) days), Customer may terminate the applicable Order(s) with respect only to those Services which cannot be provided by Cohesity without the use of the objected-to new Sub-Processor by providing written notice to Cohesity.

5.4 **Liability**. Cohesity shall be liable for the acts and omissions of its Sub-Processors to the same extent Cohesity would be liable if performing the services of each Sub-Processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 **Controls for the Protection of Customer Data**. Cohesity shall maintain appropriate physical, technical and organizational measures for protection of the security, confidentiality, and integrity of Customer Data.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1 Cohesity shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in Cohesity's or its Sub-Processors' possession of which Cohesity becomes aware (a "***Customer Data Incident***"). Cohesity shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Cohesity deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Cohesity's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1 Unless otherwise provided in the Agreement, and solely to the extent Customer Data is (i) in Cohesity's possession or (ii) cannot be deleted/retrieved by Customer, Cohesity shall on request return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement or as required by Data Protection Laws and Regulations.

9. AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates entitled to receive the Services, thereby establishing a separate DPA between Cohesity and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA (though such Authorized Affiliate may have otherwise entered the Agreement or another agreement with Cohesity). All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Cohesity under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Cohesity, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Cohesity directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Cohesity and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. EUROPEAN SPECIFIC PROVISIONS

10.1 **GDPR**. Cohesity shall Process any Personal Data subject to the GDPR in accordance with the GDPR as applicable to Cohesity's provision of its Services.

10.2 **Transfer mechanisms for data transfers**. Any transfers of Personal Data from a country subject to the GDPR under this DPA to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, shall be subject to the GDPR SCCs for the transfer of personal data to processors set forth in Schedule 2 to this DPA which are incorporated by reference herein. For the avoidance of doubt, insofar as legally required, GDPR SCCs shall also apply to any cross-border transfer of Personal Data that is subject to the laws of a country outside the EEA in which the competent authority has approved the use of the GDPR SCCs ("**Adopting Country**"), including but not limited to Switzerland. In addition, where the cross-border transfer of Personal Data is subject to the laws of the United Kingdom (including the UK General Data Protection Regulation), insofar as legally required, UK SCCs, as set out in Schedule 1, shall apply.

10.3 **Standard Contractual Clauses**.

10.3.1 Customers covered by the SCCs. The SCCs and the additional terms specified in this Section 10.3 apply to (i) the legal entity that has agreed to the SCCs as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within countries subject to the GDPR, which have entered Order(s) for or gain the benefit of the Services. For purposes of the SCCs and this Section 10.3, the aforementioned entities shall be deemed "data exporters".

10.3.2 Instructions. This DPA and the Agreement are Customer's instructions at the time of entering the Agreement to Cohesity for the Processing of Personal Data. For purposes of Clause 8.1 of the GDPR SCCs, entry into the Agreement shall be deemed Customer's express instructions to Cohesity to Process Personal Data as reasonably contemplated by the Agreement.

10.3.3 Audits and Certifications. The parties agree that the audits described in Clause 8.9 of the GDPR SCCs shall be carried out in accordance with the following specifications:

a) Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Cohesity shall make available to Customer that is not a competitor of Cohesity (or Customer's independent, third-party auditor that is not a competitor of Cohesity) information regarding Cohesity's compliance with its obligations under the Agreement and this DPA.
b) Customer may contact Cohesity in accordance with the "Notices" Section of the Agreement (or if there is no such section, by overnight courier to Cohesity's address in this DPA, marked for the attention of Cohesity's General Counsel) to request an on-site audit of the procedures relevant to the protection of Personal Data and strictly to the extent required by applicable law.
c) Before the commencement of any such on-site audit, Customer and Cohesity shall mutually agree upon the scope, timing, and methodology of the audit in addition to the reimbursement rate for which Customer shall be responsible.
d) Customer shall promptly notify Cohesity with information regarding any non-compliance discovered during the course of an audit, and all information in relation to any audit shall be treated as confidential.

10.3.4 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 16(d) of the GDPR SCCs shall be provided by Cohesity to Customer only upon Customer's request.

10.3.5 Privacy Impact Assessment and Prior Consultation. To the extent required by Data Protection Laws and Regulations and taking into account the nature of the Processing and the information available to Cohesity, Cohesity will - at Customer's request and cost - provide reasonable information to Customer to assist Customer to comply with its obligations in respect of data protection impact assessments and prior consultation under Data Protection Laws and Regulations.

10.3.6 Requests for Personal Data. If Cohesity receives a legally binding request to access Personal Data from a government body ("**Request**"), Cohesity shall to the extent permitted by applicable laws use reasonable efforts to a) promptly notify Customer and/or redirect the requesting body to make the Request directly of Customer; b) obtain confidential treatment or a protective order, and c) limit disclosure to Personal Data necessary to satisfy the Request.

10.3.7 Conflict. The terms in the Agreement and this DPA, (not including the SCCs) are, as applicable, additional clause(s) pursuant to Clause 2 of the GDPR SCCs. In the event of any conflict or inconsistency between them and the SCCs in Schedule 2, the SCCs shall prevail. In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail.

SCHEDULES

Schedule 1: SCCs
Schedule 2: Appendix to SCCs
Schedule 3: Services

SCHEDULE 1 – STANDARD CONTRACTUAL CLAUSES

PART 1 - GDPR STANDARD CONTRACTUAL CLAUSES (MODULE 2)

To the extent applicable to the Services, the European Commission's Standard Contractual Clauses for the transfer of Personal Data to Processors established in third countries (available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en) shall apply and are hereby incorporated by reference, provided:

- Module Two (Controller to Processor) will apply where Customer is a Controller and Cohesity is a Processor;
- Module Three (Processor to Processor) will apply where Customer is a Processor and Cohesity is a Processor;
- In Section I, Section 7 shall not be deemed to apply.
- In Section II of the GDPR SCCs:
    - In Clause 9, Option 2 shall apply (to the exclusion of the other Options) where Data Exporter will be informed 10 days in advance; and
    - In Clause 11(a), the Option shall not apply.
- In Section III of the GDPR SCCs:
    - In Clause 17, Option 1 shall apply (to the exclusion of the other Options), and the laws of Ireland are specified; and
    - In Clause 18(b), the courts of Ireland are specified.

The relevant Appendix is included below as Schedule 2.

For the avoidance of doubt, insofar as the transfer relates to Personal Data subject to the Data Protection Law and Regulations of an Adopting Country (such as Switzerland):

- All references in the GDPR SCCs to "Member State" will be interpreted as references to the Adopting Country and references to EU law will be interpreted as references to the relevant provisions of the laws of the Adopting Country.

- For the purposes of Clause 17, Clause 18 and Annex I.C of the GDPR SCCs, the GDPR SCCs will be governed by the data protection laws of the Adopting Country, any dispute arising from the GDPR SCCs will be resolved by the courts of the Adopting Country and the competent supervisory authority is the data protection authority of the Adopting Country.

PART 2 - UK STANDARD CONTRACTUAL CLAUSES

To the extent applicable to the Services, UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force from March 21, 2022, as officially published at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ shall apply and are hereby incorporated by reference, provided:

- For the purposes of Table 1 of the UK SCCs, the names of the parties, their roles and their details shall be set out in the attached Annex 1;

- For the purposes of Tables 2 and 3 of the UK SCCs, Module 2 of the GDPR SCCs incorporated into this DPA by reference, including the information set out in the attached Annexes, shall apply; and

- For the purposes of Table 4 of the UK SCCs, neither party may end the UK SCCs.

SCHEDULE 2 – SCC APPENDIX

Annex I

A. LIST OF PARTIES

Data exporter(s):
Name: 'Customer' defined in or identified in the Agreement
Address: Customer's address
Activities relevant to the data transferred under these Clauses: Customer's usage of the Services provided for in the Agreement.
Signature and date: Customer's authorized signatory to the Agreement
Role: Controller

Data importer(s):
Name: Cohesity, Inc.
Address: 300 Park Avenue, San Jose, CA 95110, USA
Activities relevant to the data transferred under these Clauses: Cohesity's provision of the Services provided for in the Agreement.
Signature and date: Cohesity's authorized signatory to the Agreement
Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects Whose Personal Data is Transferred
Subject to any terms in the Agreement to the contrary, Customer and Customer's Users may submit Personal Data to the Services, the extent of which is determined and controlled by Customer or Customer's User(s), as the case may be, in its and their sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's Users (who are natural persons)
- Other Data Subjects whose Personal Data is provided to Cohesity by Customer hereunder

Categories of Personal Data Transferred
Subject to any terms in the Agreement to the contrary, Customer and Customer's Users may submit Personal Data to the Services, the extent of which is determined and controlled by Customer or Customer's User(s), as the case may be, in its and their sole discretion, and which may include, but is not limited to the following categories and in each case to the extent its Personal Data:

- Information such as first and last name, date of birth, employment information (like job title or prior work history or experience), contact information (work email, work phone number, work physical address or location), and pictures
- Unique identifiers such as ID data, IP address, or other internet data
- User names/passwords

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.
Subject to any terms in the Agreement to the contrary, Customer and Customer's Users may submit special categories of data to the Services, the extent of which is determined and controlled by Customer or Customer's User(s), as the case may be, in its and their sole discretion and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of data concerning health or sex life.

The Frequency of the Transfer
Except as otherwise provided in the Agreement, Cohesity may transfer Personal Data for the duration of the Agreement on a continuous basis.

Nature of the Processing
Cohesity will Process Personal Data as reasonably contemplated by the Agreement, including Processing initiated by Users in their use of the Services and Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) consistent with the Agreement.

Purpose(s) of the data transfer and further processing
The purpose of the transfer and Processing of Personal Data by Cohesity is the performance of the Services pursuant to the Agreement, which may include, as applicable, the provision of support services under a support contract and Cohesity's use of Personal Data in connection with the sale to Customer of Hardware.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Cohesity is specifically instructed and authorized by Customer to retain Personal Data for such period of time following termination of this Agreement as reasonably necessary.

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

Details as to transfers to Sub-processors are available at https://www.cohesity.com/agreements-docs/subprocessors.pdf

C. COMPETENT SUPERVISORY AUTHORITY

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

Ireland - Data Protection Commission, or if required by law, Data Exporter's competent supervisory authority in accordance with the GDPR.

Annex II

PART A:

This Part A addresses Cohesity's approach to information security relating to:

- Cohesity support services; and
- Cohesity's organization as a whole

1. **Principles.** Cohesity emphasizes the following principles in the design and implementation of its security program and practices:
   - **1.1 Confidentiality** – Prevention of disclosure of information to unauthorized individuals or systems.
   - **1.2 Integrity** – Maintaining the accuracy and consistency of data over its life cycle.
   - **1.3 Availability** – Maximizing availability of information.
2. **Security Program.** Cohesity shall maintain an effective security program, consisting of industry best practices, which includes having:
   - **2.1** A risk management and treatment program that includes vendor risk;
   - **2.2** Conducting periodic risk assessments of systems and networks that process Customer Data on at least an annual basis. "**Customer Data**" means Customer data or Confidential Information in Cohesity's possession.
   - **2.3** Periodic review of security incidents and subsequent remediation;

2.4 A written security policy that explicitly addresses and provides guidance to its personnel in furtherance of the confidentiality, integrity and availability of Customer Data and Cohesity's systems. The policies are endorsed by Cohesity's senior management and state ramifications for noncompliance; and

2.5 Cohesity shall have resources (i.e. identified individual(s)) to foster and focus on information security efforts.

3. Data Centers.

3.1 Where Cohesity uses Data Centers (e.g. for metadata telemetry or support services) in connection with any activity under this Agreement, Cohesity shall maintain an effective security program in respect of such Data Centers, which includes using commercially reasonable efforts to ensure:

a) All activity is logged, recorded and stored for no less than 90 days;

b) Entry to each facility requires prior authorization and verification of government-issued identification and biometric confirmation;

c) Each facility has an annual audit by industry leading firms for ISO27001 and Service Organization Control compliance; and

d) Each facility includes controls regarding utilities such as power, air quality, temperature, humidity, lighting, fire suppression, and other environmental factors.

4. Cohesity's IT Security Controls

4.1 User Access, Controls and Policies. Cohesity supports a variety of security controls on its own internal information systems including:

a) centrally managed unique user identifiers (user IDs) to ensure that activities can be attributed to the responsible individual;

b) controls to revoke access upon role change or termination;

c) access review procedures;

d) strong authentication requirements;

e) denial of access to new users by default.

4.2 Cohesity Employee Access, Controls and Policies. Cohesity has implemented the following controls for Cohesity employee access to Customer systems:

a) Cohesity staff cannot access any end-user data in a Customer-controlled environment without being granted permission by the end user-owner through the native access control system;

b) Once granted by the Customer, Cohesity employee access to a Customer environment can only be obtained by authorized individuals from known networks through the mandatory use of public key infrastructure (PKI) technology;

c) Access (where granted by Customer) is based on the information security principles of 'need to know' and 'least privilege' with access strictly limited to a select number of skilled individuals;

d) employees are trained on documented information security and privacy procedures;

e) all employees are subject to employee background checks prior to employment;

f) all employees are required to sign Customer Data confidentiality agreements; and,

g) access is immediately revoked on termination of employment.

4.3 Third party service providers. Cohesity personnel take reasonable steps to select and retain only third-party service providers that will maintain and implement the security measures consistent with the measures stated in this Exhibit and in accordance with all applicable state, federal or international laws and/or regulations.

4.4 Application Controls.

a) Each facility is protected by a "defense-in-depth" security architecture consisting of firewalls, IDS (Intrusion Detection Systems), anti-virus/anti-malware protection, monitoring capabilities, and DDoS protection monitoring and mitigation;

b) The internal network infrastructure is securely segmented using firewalls, Virtual Networks (VLANS) and Access Control Lists (ACLs) which limits the access and communication between systems and environments. Systems and individuals are not permitted to reach other systems without proper authorization; and

c) Every server is hardened and imaged to contain only the necessary services to operate. All hosts are subject to a regular patching and maintenance routine and are periodically scanned for vulnerabilities and security threats using industry-leading technology. All servers are controlled and managed by an automation system to ensure consistent configuration across the environment.

5. **Vulnerability and Malware Management.** Cohesity maintains a vulnerability management program designed to identify and remediate known. Security scans are conducted on an ongoing basis.
6. **Data Encryption.** Cohesity use industry-standard encryption products to protect Customer Data in transit and at rest. All data in transit between targets and Cohesity is encrypted. Data at rest is stored in a unique nonreadable binary format and subject to AES 256-bit full disk encryption.
7. **Business Continuity and Disaster Recovery.** Cohesity conducts Business Continuity efforts to plan for the continuity and recovery of critical business systems. Plans for such activities are communicated and distributed to the appropriate teams. Such plans are tested at least annually.
8. **System Maintenance.** Maintenance is carried out during scheduled maintenance hours as provided in the Cohesity Availability and Support SLA. Maintenance is most commonly used for new version releases, typically every 4-6 weeks, but may be performed for other updates or on a different frequency.
9. **Change Management.** Cohesity manages changes through a robust set of change management procedures. All configuration changes are tracked and managed. Changes undergo a rigorous battery of tests and quality assurance. Findings are fed back into the development cycle for remediation. Promotion to release candidates and production require approvals and issuing a release is limited to a core set of individuals.
10. **Incident Management.** Cohesity maintains incident management policies and procedure describing the roles and responsibilities of the Support, IT, Security and Engineering teams and other functional groups. Escalations between the teams are determined based on the nature of issue (infrastructure, security, application or client model), duration of issue, and/or scope of issue. A root cause analysis is performed after an issue is resolved.

PART B:

If Customer uses Cohesity SaaS, this Part B applies.

1. Architecture & Data Segregation

Cohesity SaaS is a data management platform that provides a single administrative interface. Cohesity SaaS enables a Customer to manage its global data sets stored in different environments including on-premises, edge and cloud. Cohesity SaaS is designed, developed, and operated with security as a core tenet guiding our approach.

Cohesity SaaS is operated in a multitenant architecture that is designed to segregate and restrict Customer Content access. The architecture provides an effective logical data segregation for different customers uniquely implemented as an Organization. Each Organization's data and metadata are logically segregated and isolated from the other tenant Organizations via customer-specific "Organization IDs", which allows for role-based access privileges.

2. Information Security Controls

2.1. Information Security Management System

Cohesity implements an Information Security Management System ("**ISMS**") that establishes security controls to meet its objectives. The ISMS is aligned to ISO 27001 and the NIST CyberSecurity Framework. The ISMS policy and associated controls are reviewed no less than once per annum.

2.2 Data Encryption

Customer Content and Service Analytics Data is encrypted at rest using AES-256, and the encryption keys are managed in a key management system (KMS). All Customer Content and Service Analytics Data in-transit over untrusted networks use Transport Layer Security (TLS) 1.2 (or better).

2.3 Access Management

a) Cohesity Access Controls:

Cohesity SaaS implements identity and access management ("**IAM**") controls to manage access to Cohesity SaaS infrastructure. Access is provided on a principle of least privilege and separation of duties. A unique user ID and multi-factor authentication are required for all Cohesity access to Cohesity SaaS infrastructure. The infrastructure on which Cohesity SaaS is hosted is accessed only by Cohesity-authorized personnel.

b) Cohesity Personnel:

Cohesity requires certain background screening on its personnel as a part of its hiring process (to the extent permitted by applicable law). In addition, all Cohesity employees are subject to confidentiality agreements protecting nonpublic information they access in the course of their employment, and attend internal security training appropriate to their role within Cohesity.

c) Access Reviews:

Cohesity reviews the access privileges of its personnel at least annually, and disables access by separated personnel on a timely basis.

d) Organization Access Controls:

Cohesity SaaS provides a Customer admin user with IAM controls to manage user accounts and assign appropriate access in accordance with that Customer's security standards and policies. Customers can, if they choose, integrate Cohesity SaaS with an authorization and identity provider to protect privacy and secure access.

2.4 Monitoring

Monitoring tools or services, including key performance indicators and metrics, are utilized by Cohesity to track certain activities and changes within Cohesity SaaS. Dashboards and metrics are tracked and evaluated by the appropriate Cohesity operations team.

3. Infrastructure Defenses

Cohesity shall implement reasonable measures designed:

(i) to protect against distributed denial of service (DDOS), intrusion, and malware attacks on Cohesity SaaS Infrastructure, including:

a) firewalls to monitor connections;
b) evaluation and blocking of anomalous connections into the Cohesity SaaS environment;
c) monitoring servers, containers, and infrastructure for vulnerabilities;
d) addressing discovered vulnerabilities on a regular, systematic basis, and

(ii) to ensure that Cohesity SaaS will not transmit to Customer any malware, viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, disabling code, trap door devices or other malicious programs or instructions intended to erase, corrupt or modify any data, programs, or information, or bypass internal or external Customer security measures for the purpose of gaining unauthorized access.

4. Secure Development Life Cycle

Cohesity adheres to secure development lifecycle principles designed to eliminate security vulnerabilities and ensure delivery of securely developed products to Customers. In particular, Cohesity practices:

1. Security training
2. Security in design
3. Threat model in architecture
4. Vulnerability management
    - Vulnerability management policy
    - Penetration testing
    - Static code and binary analysis
    - Dynamic scanning
    - Third-party component security

- Support for product infrastructure and tools

5. Secure product release
6. Product incident response

5. Incident Response

Cohesity maintains security incident management policies and procedures. Cohesity will notify (without undue delay) impacted Customers of any unauthorized disclosure of Customer Content of which Cohesity becomes aware.

6. Service Analytics Data

Cohesity uses reasonable measures designed to ensure that (with the exception of Customers using Cohesity Data Plane) Cohesity SaaS does not store, process or otherwise handle Customer Content. Cohesity may use, process or store Service Analytics Data in relation to Cohesity SaaS subject to and in accordance with the Cohesity SaaS Terms of Service.

7. Compliance & Certifications

Cohesity maintains certain certifications and adheres to certain standards described at https://www.cohesity.com/security-and-trust/. Cohesity may update this Annex II from time to time by posting updated terms on www.cohesity.com/agreements, provided that no such update will materially adversely diminish Cohesity's obligations hereunder.

SCHEDULE 3 – SERVICES

1. Cohesity SaaS