DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("Addendum") forms part of the Master Customer Agreement (or other similarly titled written or electronic agreement addressing the same subject matter) between Druva and Customer for the purchase of data management cloud products and services from Druva ("Cloud Services"), wherein such agreement is hereinafter defined as the "Customer Agreement," and whereby this Addendum reflects the parties' agreement with regard to the Processing of Personal Data. In the event of any conflict between the terms of this Addendum and the terms of the Customer Agreement with respect to the subject matter herein, this Addendum shall control. All capitalized terms not defined in this Addendum shall have the meaning given to them in other parts of the Customer Agreement.

NOW THEREFORE, the parties agree as follows:

1. Definitions

1.1 For purposes of this Addendum, each of the following terms shall have the meaning set forth below:

(a) "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, as amended by the California Privacy Rights Act, and its implementing regulations, as amended or superseded from time to time.

(b) "Customer Agreement" means the Order Form or any executed agreement between Customer and Druva (if any) for the purchase of the Cloud Services.

(c) "Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data, and if applicable, includes "Business" as defined under CCPA. For purposes of this Addendum, Data Controller is Customer and its Authorized Users (if applicable).

(d) "Data Processor" means the natural or legal person, public authority, agency, or other body which alone or jointly with others, Processes Personal Data on behalf of the Data Controller, and if applicable, includes "Service Provider" as defined under CCPA. For purposes of this Addendum, Data Processor is Druva.

(e) "Data Subject" means an identified or identifiable natural person to whom Personal Data relates and if applicable, includes a "Consumer" as defined under CCPA.

(f) "Data Protection Law" means all laws and regulations applicable to the Processing of Personal Data under the Customer Agreement, including those of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, each as applicable, and as may be replaced from time to time.

(g) "Druva" has the meaning set forth in the Customer Agreement.

(h) "Druva Affiliates" means the Druva corporate entities listed in Annex III excluding Druva as defined above.

(i) "EEA" means the European Economic Area.

(j) "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

(k) "International Data Transfer" means any disclosure of Personal Data by an organization subject to Data Protection Law to another organization located outside the EEA, the UK or Switzerland, where such disclosure is restricted by the applicable Data Protection Law.

(l) "Member State" means a member state of the European Union or the EEA.

(m) "Personal Data" means any information relating to a Data Subject that meets the definition of the same or similar term (such as "Personal Information" or "Personally Identifiable Information") under applicable Data Protection Law that is uploaded by or for Customer or Customer's agents, employees, affiliates, or contractors to the Cloud Services as part of Customer Data.

(n) "Process" or "Processing" has the meaning under applicable Data Protection Law, or where no such term exists, means any operation or set of operations which is performed upon Personal Data, whether or not by automated 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.

(o) "Security Incident" means a breach of security leading to the unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

(p) "Standard Contractual Clauses" means:

1. the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021, for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council (or any updated version thereof) ("EEA SCCs"); and
2. the addendum to the EEA SCCs issued by the UK Information Commissioner under Section 119(A)(1) of the UK Data Protection Act 2018 ("DPA 2018") (version B1.0, in force March 21, 2022) (or any updated version thereof) (the "UK Addendum").

(q) "Third-Party Data Controller" means a Data Controller for which Customer is a Data Processor.

2. Provision of the Cloud Services. Druva shall provide Cloud Services to Customer in accordance with the Customer Agreement. In connection with the Cloud Services, the parties agree to Druva Processing Customer Data that may contain Personal Data.

3. Processing Purposes, Scope, and Customer's Processing Instructions.

3.1 General. Druva shall only Process Personal Data in accordance with Customer's instructions and to the extent necessary for providing the Cloud Services as described in the Customer Agreement, which constitutes a business purpose under CCPA. The type of Personal Data that will be Processed by Druva and the duration of the Processing of that Personal Data will be identified in the Customer's instructions, located in Annex I, unless otherwise agreed. Druva will never sell Customer Data.

3.2 CCPA To the extent CCPA applies, the parties acknowledge that Druva is a "Service Provider" as that term is defined under CCPA and that Customer's transfer of any Personal Data to Druva is not a sale, and Druva provides no monetary or other valuable consideration to Customer in exchange for Personal Data. Except as otherwise instructed by Customer, Druva shall not (a) sell or share Personal Data or (b) collect, retain, use, or disclose Personal Data for any purpose (including any commercial purpose) other than for the specific purpose of providing the Cloud Services under the Customer Agreement or as otherwise permitted by CCPA. The Customer Agreement, this Addendum and any additional data processing instructions provided by Customer shall constitute "instructions," so long as any additional or alternate instructions are consistent with the purpose and scope of the Customer Agreement and are provided and/or confirmed in writing by the Customer. Druva shall immediately notify Customer if an instruction, in Druva's opinion, infringes the Data Protection Law. Druva shall also notify Customer if it makes a determination that it can no longer meet its obligations under the Data Protection Law, at which point Customer shall have the right to take reasonable and appropriate measures to stop and remediate any unauthorized use of Personal Data.

4. Data Processor Personnel. Druva shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements. Druva shall ensure that Druva's access to Personal Data is limited to those personnel assisting in the provision of the Cloud Services in accordance with the Customer Agreement.

5. Customer Responsibilities. Customer shall, in its use of the Cloud Services, Process Personal Data in accordance with the requirements of Data Protection Law and shall ensure that its instructions for Processing of Personal Data are compliant with the Data Protection Law, and if applicable, CCPA. Customer represents and warrants that it has provided any required notice that the Personal Data is being used or shared consistent with applicable Data Protection Law.

6. Data Subject Requests.

6.1 GDPR**.** Druva shall promptly notify Customer if Druva receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). To the extent Customer cannot do so on its own, Druva shall assist Customer by appropriate organizational and technical measures for the fulfilment of Customer's obligation to respond to and address Data Subject Request under the Data Protection Law. Customer shall be responsible for any costs arising from Druva's provision of such assistance that is beyond the scope of Druva's standard support included with the provision of the Cloud Services.

6.2 CCPA. Druva shall provide reasonable assistance to Customer for the fulfilment of Customer's obligation to respond to and address requests of Data Subjects who are consumers under CCPA relating to rights provided by CCPA. Customer shall be responsible for any costs arising from Druva's provision of such assistance that is beyond the scope of Druva's standard support included with the provision of the Cloud Services. Druva shall not be required to delete any of the Personal Data to comply with a request to exercise

CCPA rights directed by Customer if it is necessary to maintain such information in accordance with Cal. Civ. Code 1798.105(d), in which case Druva shall promptly inform Customer of the exceptions relied upon under 1798.105(d) and Druva shall not use the Personal Data retained for any other purpose than provided for by that exception.

6.3 Other Data Protection Law. Druva shall promptly notify Customer if Druva receives a request from a Data Subject to exercise the Data Subject's rights as articulated under the applicable Data Protection Law, Druva shall assist Customer by appropriate organizational and technical measures, to the extent possible, for the fulfilment of Customer's obligation to respond to and address the Data Subject's request under the Data Protection Law. Customer shall be responsible for any costs arising from Druva's provision of such assistance that is beyond the scope of Druva's standard support included with the provision of the Cloud Services.

7. **Deletion of Personal Data.** Upon termination or expiration of the Customer Agreement, Druva shall return and/or delete Customer Data, including Personal Data contained therein, pursuant to the terms of the Customer Agreement. Druva will provide a certificate of deletion upon Customer's request.

8. **Data Security Measures.** Druva shall employ the security measures set forth in Annex II.

9. **Sub-Processors.** Customer authorizes Druva to engage sub-Data Processors ("Sub-Processor") appointed in accordance with this Section 9. Druva's engagement of any Sub-Processor shall be pursuant to a written contract binding the Sub-Processor to observe all requirements under applicable Data Protection Law, and Druva will be liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Druva. Upon written request of the Customer, Druva will provide to Customer an up-to-date list of its current Sub-Processors, the current version of which, including Druva Affiliates, is in Annex III. Customer acknowledges that (a) Druva's Affiliates may be retained as Sub-Processors and (b) Druva and Druva Affiliates may engage third-party Sub-Processors in connection with the provision of the Cloud Services, including the Cloud Providers listed in Annex III. Druva shall notify Customer in writing of any new Sub-Processor. Where the Standard Contractual Clauses do not apply, Customer may exercise its right to object to the use of the new Sub-Processor by notifying Druva in writing within ten (10) business days after receipt of Druva's notice by emailing privacy@druva.com; where the Standard Contractual Clauses apply, refer to Section 14.2 of this Addendum for the time period for the right to object. In the event Customer objects to a new Sub-Processor, and that objection is based on reasonable grounds that such Sub-Processor is unable to protect Customer Data in accordance with the terms of the Agreement and this Addendum, Druva will use reasonable efforts to make available to Customer a change in Cloud Services. If Druva is unable to make available such change within a reasonable time period, Customer may terminate the applicable Order Form(s) by providing a written notice to Druva.

10. **Requests from Authorities.** In the case of an audit, inquiry, or investigation by a government body, data protection authority, or law enforcement agency regarding the Processing of Personal Data, Druva shall promptly notify Customer unless prohibited by applicable law. For the avoidance of doubt, the Addendum will not require Druva to pursue any action or inaction that could result in civil or criminal penalty for Druva such as contempt of court.

11. **Security Incident.** In the event of a Security Incident, Druva shall respond as detailed in Section XII of Annex II.

12. **Liability.** Each party's and all of its Affiliates' liability arising out of or related to this Addendum, whether in contract, tort, or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Customer Agreement. Druva's and its Affiliates' total liability for all claims from the Customer and all of Customer's Affiliates shall apply in the aggregate for all claims under the Customer Agreement and the Addendum.

13. **Audits.** Upon Customer request, Druva will provide to Customer annually an opinion or report provided by an accredited, third-party audit firm under the Statement on Standards for Attestation Engagements No. 18 SOC 2 review ("SOC II Audit") and/or under International Information Security Standard ISO 27001 certification ("ISO 27001 Certification") (each SOC II Audit and ISO 27001 Certification a "Report"). If a Report does not provide, in Customer's reasonable judgment, sufficient information to confirm Druva's compliance with the terms of this Addendum or with applicable Data Protection Law, then Customer or an accredited third-party audit firm agreed to by both Customer and Druva may audit Druva's compliance with the terms of this Addendum and applicable Data Protection Law during regular business hours with reasonable advance notice to Druva and subject to reasonable confidentiality procedures. Customer will be responsible for all costs and fees related to such audit, including reasonable costs and fees for any and all time Druva expends for any such audit. Before commencement of any such audit, Customer and Druva shall mutually

agree upon the scope, timing, and duration of the audit. Customer shall promptly notify Druva with information regarding any non-compliance discovered during the course of an audit and all audit findings regarding Druva will be the Confidential Information of Druva. Customer may not audit Druva more than once annually.

14. International Data Transfers.

14.1 Transfers. The parties agree that Personal Data Processed under this Addendum may be transferred outside the EEA, Switzerland or the UK as necessary to provide the Cloud Services, in which case appropriate safeguards will be implemented for the transfer of Personal Data in accordance with Data Protection Law. If Personal Data Processed under this Addendum is transferred from the EEA or Switzerland to a jurisdiction for which the European Commission has not issued an adequacy decision, the EEA SCCs shall apply. If Personal Data Processed under this Addendum from the UK to a jurisdiction for which adequacy regulations have not been adopted by the Secretary of State under the DPA 2018, the UK Addendum shall apply.

14.2 International Data Transfers outside the EEA and Switzerland. By signing this Addendum, Customer and Druva conclude Module 2 (Controller to Processor) of the EEA SCCs, and, to the extent Customer is a Data Processor on behalf of a Third-Party Data Controller, Module 3 (Processor-to-Subprocessor) of the EEA SCCs, which are hereby incorporated and completed as follows: the "data exporter" is Customer; the "data importer" is Druva; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented, the time period is ten (10) days and Customer acknowledges that Druva engages the Sub-Processors listed in Annex III; the optional redress clause in Clause 11(a) is struck; Option 1 of Clause 17 is implemented and the governing law is the law of the Data Exporter (and if none applies, then the law of Ireland); the courts in Clause 18(b) are the Courts of the Member State in which Customer is established; Annex I, Annex II and Annex III to the SCCs are Annex I, Annex II and Annex III to this Amendment respectively. For International Data Transfers from Switzerland: (i) Data Subjects who have their habitual residence in Switzerland may bring claims under the SCCs before the courts of Switzerland and (ii) the SCCs cover Personal Data pertaining to legal entities until the entry into force of the revised Swiss Federal Act on Data Protection Act of 2020.

14.3 International Data Transfers outside the UK. By signing this Addendum, Customer and Druva conclude the UK Addendum which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Druva, their details are set forth in this Amendment and the Customer Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 14.2 of this Amendment; (iii) in Table 3, Annex I (A and B), Annex II and Annex III to the "Approved EU SCCs" are Annex I, Annex II and Annex III to this Amendment respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

14.4 Compliance. If Druva's compliance with Data Protection Law applicable to Standard Contractual Clauses is affected by circumstances outside of Druva's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then Customer and Druva will work together in good faith to reasonably resolve such non-compliance.

15. Customer Compliance Documentation. Upon Customer's request, Druva will provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Cloud Services to the extent Customer does not have access to such information without Druva's assistance.

The signatures of the authorized individuals of the parties below confirm that this is a valid and binding Addendum effective as of the date of full execution below by the parties.

Druva	**Customer:**
Signature:	**Signature:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s): Customer of Druva using Druva Cloud Services for data management, storage, and backup.

Data importer(s): *Druva and Druva Affiliates as applicable*
Contact person's name, position and contact details: Hsinya Shen, DPO, privacy@druva.com
Activities relevant to the data transferred under these Clauses: Provision of enterprise cloud computing solutions which processes Personal Data within Customer Data through its Cloud Services.

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred: All Data Subjects included in the Customer Data, the extent of which is determined and controlled by Customer and Customer Affiliates in their sole discretion, including: prospective, current, and former employees; independent contractors (who are natural persons); representatives of vendors and suppliers; and clients.

Categories of personal data transferred: All Personal Data elements and categories included in the Customer Data, the extent of which is determined and controlled by Customer and Customer Affiliates in their sole discretion.

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.: All sensitive data included in the Customer Data, the extent of which is determined and controlled by Customer and Customer Affiliates in their sole discretion.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Data is transferred on an ongoing basis for the term of the Customer Agreement. Data exporter chooses frequency at which data is backed up through the Cloud Services.

Nature of the processing: To perform Cloud Services pursuant to the Customer Agreement.

Purpose(s) of the data transfer and further processing: The Personal Data will be transferred and further processed for the provision of the services as described in the Customer Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Until Data is deleted in accordance with section 7 of this Addendum.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: For the subject matter and nature of the Processing, reference is made to the Customer Agreement and this Addendum; the Processing will take place for the duration of the Customer Agreement.

C. **COMPETENT SUPERVISORY AUTHORITY**

Clause 13 shall apply as follows: Where Customer is established in an EU Member State, the United Kingdom, Switzerland, or has appointed an Article 27(1) representative, the supervisory authority shall be the regulator where Customer is established, or has appointed a representative, as applicable, otherwise Ireland's Data Protection Commission shall apply.

ANNEX II

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

This Annex II governs the manner in which Druva shall handle Customer Data.

I. **Information Security Program:** Druva shall maintain a written information security program including documented policies, standards, and operational practices that meet the applicable security requirements, and controls set forth in this Exhibit to the extent applicable to the Cloud Services and identify an individual within the organization responsible for its enforcement. Druva shall have processes and procedures in place so that information security events may be reported through appropriate communications channels as quickly as possible. All employees, contractors and third-party users shall be made aware of their responsibility to report any breach of security leading to the unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data ("Security Incident") as quickly as possible.

II. **Customer Data Protection:** Druva shall adopt, administrative, technical and physical measures designed to preserve the confidentiality, integrity and accessibility of Customer Data, that conform to best practices that Druva then applies to its own processing environment and generally recognized industry standards. Maintenance of a secure processing environment includes but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by Druva.

III. **Cloud Operations:** Prior to gaining access to administer the Druva Cloud Services, Druva cloud operations personnel will undergo appropriate background checks. Access to the Druva Cloud Operations environment will be based on the principle of least privilege and be assigned on demonstrated and legitimate need to know basis. Druva will perform access control review of Druva employees managing day to day operation of the Cloud Services.

IV. **Application Security:** Druva shall at all times develop, provide, maintain and support Cloud Services and the software and subsequent updates, upgrades and bug fixes such that the Cloud Services and the software remain secure from those vulnerabilities as described in The Open Web Application Security Project's (OWASP) "Top Ten Project" and other generally recognized and comparable web application security standards.

V. **Network Security:** Druva shall at all times maintain appropriate network security to protect Customer Data. Such measures shall include at a minimum network firewall provisioning, intrusion detection and annual third-party vulnerability assessments.

VI. **Security Logging and Monitoring:** Druva will implement logging systems and log reviews reasonably sufficient to detect security issues such as loss, misuse, or unauthorized access to Customer Data. This will include developing a baseline of expected activity within the Cloud Services; logging to detect activity exceeding baseline thresholds. Logs shall be regularly reviewed by Druva, either manually or using log parsing tools. Logs will be retained for a minimum of six (6) months and protected from unauthorized access, modification, and accidental or deliberate destruction.

VII. **Encryption:** Druva agrees to encrypt Customer Data with industry best practice encryption levels at all times while in transit over a public network or wireless network and while stored in the cloud service.

a. **Data in Flight:** Druva agrees to encrypt Customer Data in transit to the Druva Cloud Service using industry best practices such as Transport Layer Security or equivalent.

b. **Data at Rest:** Druva agrees to encrypt Customer Data at rest in the Druva Cloud Service using industry best practices of a unique Advanced Encryption Standard (AES) encryption key or equivalent per customer. This unique encryption key per customer will provide logical and cryptographic segmentation of Customer Data.

VIII. **Software Development Lifecycle**

a. **Vulnerability Management:** As part of Druva's software development lifecycle, Druva will implement a "Vulnerability"[1] management plan such that:

[1] Vulnerability" shall be defined as a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.

Vulnerability Rating	Classification	Mitigation
Critical	can readily be compromised with publicly available malware or exploits.	14 days from discovery
High	no current or known publicly available malware or exploits available.	30 days from discovery
Medium	can be mitigated within an extended timeframe	90 days from discovery
Low	not easily exploited or have minimal if any impact.	180 days from discovery

b. **Environment Segmentation:** Druva agrees to maintain segmented environments between production and development environments. Given Druva's envelope encryption model[2], Druva will not and cannot use Customer Data in those development environments.

IX. **Third-Party Penetration Testing:** Druva shall engage a qualified third party to perform annual penetration testing of the Cloud Services where Customer Data is stored. The scope of the penetration testing will include all internal/external systems, devices and applications that are used to process, store, transmit Customer Data, and social engineering tests. Summary results can be provided to the customer under a Non-Disclosure Agreement.

X. **Cloud Provider**

a. **Relationship between Druva and Cloud Provider(s):** Druva uses cloud provider(s) to supply cloud infrastructure that Druva uses to provide Cloud Services ("Cloud Providers"). The Cloud Provider's infrastructure includes the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. The Cloud Provider's infrastructure is designed and managed according to security best practices.

b. **Physical Security:** Cloud Provider's data centers are housed in nondescript facilities with strictly controlled physical access both at the perimeter and at building access point by 1) intrusion detection systems, 2) professional security staff, 3) video surveillance and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. All physical access to data centers by Cloud Provider's employees is logged and audited routinely.

c. **Certifications:** The IT infrastructure of Cloud Provider(s) is in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 18/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- MTCS Level 3
- FIPS 140-2 (Gov Cloud only)
- FISMA, DIACAP, and FedRAMP (Gov Cloud Only)

d. **Asset Disposal and Reclamation:** When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent Customer Data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

[2] Envelope encryption is the practice of encrypting data with a data encryption key (DEK) and then encrypting the DEK with a key encryption key (KEK) that is managed by the Customer.

XI. **Certifications, Attestations, and Assessments:** Upon Customer's request, Druva shall provide a general Service Organization Control ("SOC") 2, Type II audit report. If such report(s) include(s) any findings that Druva fails to comply with the SOC 2 requirements, or audit tests result in exceptions, Druva agrees to remedy such noncompliance within a reasonable time. Any gaps will be covered by Bridge Letters[3].

XII. **Security Incident Response:** Upon confirming that a Security Incident occurred, Druva shall without undue delay: (1) taking into account the nature of Druva's Processing of Personal Data and the information available to Druva, notify the Customer; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain, investigate, and mitigate the Security Incident. Druva shall reasonably cooperate with Customer in any post Security Incident communication efforts.

XIII. **Business Continuity:** Druva shall maintain a business continuity plan and business continuity testing procedures, which include but are not limited to the areas of disaster recovery planning and data security. Druva shall review, update, and test the business continuity plan annually.

ANNEX III

LIST OF SUB-PROCESSORS

The following is the current list of Sub-Processors:

1.Name: Amazon Web Services
Address: 410 Terry Avenue North, Seattle, WA 98109, United States
Description of processing: Hosting Provider

LIST OF DRUVA AFFILIATES

The following are Druva Affiliates that may act as Sub-Processors (per Section 9):

Name of Entity	Registered Address	Subprocessor Role:
Druva Singapore Pte. Ltd.	600 North Bridge Road, Parkview Square #10- 01, Singapore, 188778	None unless this Druva entity is performing technical services, Customer support services, or supporting the provision, management and maintenance of the Products or Services.
Druva Data Solutions Private Limited	8th & 9th Floor, The Pavilion Senapati Bapat Marg Pune, India 411016	
Druva Europe Limited	6th Floor, 9 Appold Street, London, United Kingdom, EC2A 2AP	
Druva GmbH	Kasinostraße 19, 42103 Wuppertal, Germany	
Druva Inc.	2051 Mission College Blvd., Santa Clara, CA 95054	
Silver Lining Cloud Consulting Limited t/a CloudRanger	Unit 17, Colab, LYIT, Port Road, Letterkenny, Co. Donegal, F92 XFR1	

[3] A letter from a third-party service auditor stating that no changes have been made since the last type 1 or type 2 report under SSAE 18 SOC report.