DATA PROCESSING ADDENDUM

Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2010/87/EU – Standard Contractual Clauses (Processors)

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the California Consumer Privacy Act of 2018 effective January 1, 2020 and its implementing regulations, as amended or superseded from time to time.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 and if applicable, includes a "Consumer" as defined under CCPA.

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

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

(h) "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 "GDPR" and any applicable national laws made under the GDPR, the EU Directive 2002/58/EC (the "ePrivacy Directive"), the United Kingdom Data Protection Act 2018, and any regulation superseding any of the foregoing.

(i) "Process" or "Processing" 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.

(j) "Personal Data" means any information relating to a Data Subject uploaded by or for Customer or Customer's agents, employees, affiliates, or contractors to the Cloud Services as Customer Data, and if applicable, includes "Personal Information" as defined under CCPA.

(k) "Standard Contractual Clauses" means Exhibit A attached to this Addendum pursuant to the European Commission Decision on 5 February 2010 on standard contractual clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of protection (or any updated version thereof).

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.** 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. To the extent CCPA applies, the parties acknowledge 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, Provider is prohibited from (a) selling the Personal Data or (b) collecting, retaining, using or disclosing the Personal Data for any purpose (including any commercial purpose) other than for the specific purpose of providing the Cloud Services under the Customer Agreement, including as described in Section 3(d)(*Usage and Configuration Metrics*), or as otherwise permitted by CCPA. Druva shall not further collect, sell, or use Personal Data except as necessary to perform the Cloud Services under the Customer Agreement. For the avoidance of doubt, Druva shall not use the Personal Data for the purpose of providing services to another person or entity, except that Druva may combine Personal Data received from one or more entities to which it provides similar services to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity. 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 EU Data Protection Law.

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 EU Data Protection Law and shall ensure that its instructions for Processing of Personal Data are compliant with the EU Data Protection Law, and if applicable, CCPA. Customer represents and warrants that it has provided notice that the Personal Data is being used or shared consistent with Cal. Civ. Code 1798.140(t)(2)(C)(i).

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"). 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 Data Subject Request under the EU Data Protection Law. Customer shall be responsible for any costs arising from Druva's provision of such assistance.

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. 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.

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 maintain appropriate technical and organizational safeguards and reasonable security measures and practices to protect the security, confidentiality and integrity of Customer Data, including any Personal Data contained therein, as described in Exhibit C. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction.

9. **Sub-processors.** Customer authorizes Druva to engage Sub-Processors appointed in accordance with this Section 9 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 a list of its then-current Sub-Processors. 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 Cloud Providers. Druva shall notify Customer in writing of any new Sub-Processor. 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 . In the event Customer objects to a new Sub-Processor, and that objection is reasonable, 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.** Notwithstanding any provision to the contrary of the Customer Agreement or this Addendum, Druva may cooperate with law enforcement agencies concerning conduct or activity that it reasonably and in good faith believes may violate federal, state, or local law. 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. Customer shall cooperate and provide all necessary information and records to Druva in the event Druva is required to produce any records of Personal Data Processed by Druva to a data protection authority. Customer shall reimburse Druva for any reasonable costs incurred in connection with the fulfilment of Druva's obligations under this section.

11. **Incident Response.** Druva shall report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data that it becomes aware of without undue delay.

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 thirty (30) days prior written notice, Customer or a security audit firm on behalf of Customer may audit Druva and Druva's Affiliates that provide service for the Processing or transport of Customer Data. Any such audit shall be subject to confidentiality obligations, and any Confidential Information or commercially sensitive information shall be redacted. If Druva has an external audit firm perform an SSAE 16 SOC 2 review, Customer will have the right to review the controls tested and the results, and Druva shall deliver such SOC 2 report to Customer upon request. Audits will be at Customer's sole expense, except where the audit reveals material noncompliance with contract specifications, in which case the audit costs will be borne by Druva. Any findings under such audit shall constitute Druva's Confidential Information. Audits shall not occur more than once every twelve (12) months unless required by the instruction of an EU data protection authority, or the Customer believes a further audit is necessary due to material noncompliance with contract specifications. If the parties have entered into Standard Contractual Clauses as described in Section 14 (International Data Transfers), the parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section 13.

14. **International Data Transfers.**

14.1 Transfers. The parties agree that Druva may transfer Personal Data Processed under this Addendum outside the EEA, Switzerland or the United Kingdom as necessary to provide the Cloud Services. If Druva transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Druva will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with EU Data Protection Law; or rely on the Standard Contractual Clauses referred to in Section 14.3.

14.2 Sub-Processors. Druva shall require Sub-Processors to abide by the Standard Contractual Clauses for Data Processors established in third countries or another lawful mechanism for the transfer of Personal Data as approved

by the European Commission

14.3 Druva. Druva shall comply with the Standard Contractual Clauses (executed between the parties in Exhibit A) with respect to transfers of Personal Data from the EEA or the United Kingdom.

14.4 Compliance. If Druva's compliance with EU 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. Data Protection Impact Assessments. 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 authorized individuals of the parties below confirm that this is a valid and binding Addendum effective as of the date of full execution by the parties.

Druva

DocuSigned by:
By: Jung-Kyu K. McCann
821B16D1F872459...

Name: Jung-Kyu K. McCann.

Title: General Counsel

Date: 12/3/2019

[Insert Customer Name]

By: _____

Name: _____

Title: _____

Date: _____

Exhibit A

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

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

Customer
(the data**exporter**)

Druva
(the data **importer**)
each a "party"; together "the parties",

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

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

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

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

Clause 2

Details of the transfer

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

---

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

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

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

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

(e) that it will ensure compliance with the securitymeasures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

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

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

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

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

---

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
Customer of Druva using Druva Cloud Services for data management, storage, and backup.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
Druva Inc., a provider of enterprise cloud computing solutions which processes Personal Data and customer data through its Cloud Services and requires the transfer of metadata to the US (namely application logs, debugging logs, and configuration settings).

Data subjects
The personal data transferred concern the following categories of data subjects (please specify): Data subjects include but is not limited to: prospective, current, and former employees; independent contractors (who are natural persons); representatives of vendors and suppliers; and clients.

Categories of data
The personal data transferred concern the following categories of data (please specify): Data relating to but is not limited to: prospective, current, and former employees; independent contractors (who are natural persons); representatives of vendors and suppliers; and clients. Such data includes: first and last name; nickname; contact information, including residential and work mailing addresses, telephone numbers, email addresses, and emergency contact information; general financial information; number of dependents; nationality; date of birth; national ID number and/or social security number; hire date, place of executing the employment, and department of employment; job title, job category, job status, and supervisor; education and certifications and training; standard weekly hours, overtime, holiday entitlement, and information regarding compensation, benefits, and employee stock ownership; performance evaluations; workers' compensation, disability accommodation administration information and physician notes not containing health information; and termination date and reason. Metadata gathered through the use of the services, namely application logs, debugging logs, and configuration settings'.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify): Data Exporter may submit data, which includes: personal health information, such as disability status, collected for government reporting purposes; religious affiliation, collected for purposes of determining and deducting the legally required church tax from compensation; criminal history information, collected as permitted by applicable law for purposes of evaluating job applicants; and trade union membership, collected for purposes of deducting union dues from compensation.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):The purpose of processing the Personal Data by data importer is to perform Cloud Services pursuant to the Customer Agreement.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

List of Druva Companies

Name of Entity	Registered Address
Druva Holdings, Inc.	800 W. California Avenue, Suite 100, Sunnyvale, CA 94086
Druva Singapore Pte. Ltd.	600 North Bridge Road, Parkview Square, #10-01, Singapore 188778
Druva Inc.	800 W. California Avenue, Suite 100, Sunnyvale, CA 94086
Druva Europe Limited	450 Brook Drive, Green Park, Reading RG2 6UU, UK
Druva GmbH	Kasinostrasse 19-21, 42103 Wuppertal, Germany
Druva Goda Kaisha	3rd Floor of Otemachi Financial City Grand Cube, 9-2, Otemachi 1-chrome, Chiyoda-ku, Tokyo, Japan
Druva Data Solutions Private Limited	8th & 9th Floor, The Pavilion Senapati Bapat Marg Pune, India 411016
Silver Lining Cloud Consulting Limited t/a CloudRanger	Unit 17, Colab, LYIT, Port Road, Letterkenny, Co. Donegal, F92 XFR1

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Druva's Security Exhibit is attached as Exhibit C

Exhibit C

Druva Information Security Exhibit

This Druva Security Exhibit ("Exhibit") governs the manner in which Druva and Druva's Cloud Provider(s) 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 unauthorized access to, loss, or exposure of 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 or open source support.

III. Cloud Operations

Prior to gaining access to administrate the Druva Cloud Service, Druva Cloud Operations personnel will undergo appropriate background checks. Access to the Druva Cloud Operations environment will be based on the principle of least privileged 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 ("Cloud Operations Personnel") on a monthly basis.

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 information 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[4] management plan such that:

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	60 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 products and development environments. Given Druva's Envelope Encryption Model[5], Druva will not and cannot use Customer Data in those development environments.

IX. Third-Party Penetration Testing

[4] 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.

[5] 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.

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) that supply cloud infrastructure that Druva uses to provide Cloud Services. 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 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP (Gov Cloud Only)
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2 (Gov Cloud only)
- MTCS Level 3

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.

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 Provider fails to comply with the SOC 2 or SOC1/SSAE 16 requirements, or audit tests

result in exceptions, Druva agrees to remedy such noncompliance within reasonable time. Any gaps will be covered by Bridge Letters[6].

XII. Security Incident Response

Druva shall without undue delay from discovery notify Customer of any Security Incident and will promptly coordinate with Customer to investigate and remedy such Security Incident in a diligent and timely manner. Unless required by the applicable law, Druva agrees not to inform any third party of any Security Incident, without Customer's prior written consent. If such disclosure is required by applicable law, Druva agrees to work with Customer, at no additional cost to Customer, regarding the content of such disclosure to minimize any potential adverse impact on Customer. Druva's obligation to report or respond to a Security Incident Breach will not be construed as an acknowledgement by Druva of any fault or liability with respect to the Security Incident.

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.

[6] 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 16 SOC report.