# ExaVault Data Processing Addendum

This Data Protection Addendum ("**Addendum**") forms part of the Terms of Use ("**Terms of Use**") between: (i) ExaVault, Inc., a California corporation ("**ExaVault**") and (ii) "Customer" as that term is defined in the Terms of Use acting on its own behalf and as agent for each Customer Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Terms of Use. Except as modified below, the terms of the Terms of Use shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Terms of Use to govern processing by ExaVault of any Customer Data that is subject to the EU General Data Protection Regulation. Except where the context requires otherwise, references in this Addendum to the Terms of Use are to the Terms of Use as amended by, and including, this Addendum.

## 1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any EU Customer Personal Data in respect of which any Customer or its Affiliates is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any EU Customer Personal Data in respect of which any Customer or its Affiliates is subject to any other EU Data Protection Laws;

1.1.2 "**Customer Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the

management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**EU Customer Personal Data**" means any Personal Data Processed by ExaVault on behalf of a Customer, its Affiliates, agents, or customers, pursuant to or in connection with the Terms of Use, where such Personal Data is subject to the EU Data Protection Laws;

1.1.4 "**EEA**" means the European Economic Area;

1.1.5 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.6 "**GDPR**" means EU General Data Protection Regulation 2016/679; 1.1.7 "**Restricted Transfer**" means:

1.1.7.1 a transfer of EU Customer Personal Data from any Customer or its Affiliates to ExaVault; or

1.1.7.2 an onward transfer of EU Customer Personal Data from ExaVault to a subprocessor,

in each case, where such transfer would be prohibited by EU Data Protection Laws in the absence of the Standard Contractual Clauses to be established under section 11.1; however, for the avoidance of doubt, transfers pursuant to the US-EU Data Privacy Shield, or any successor or similar program that obviates the need for the Standard Contractual Clauses, are not Restricted Transfers;

1.1.8 "**Services**" means the services described in section 2 of the Terms of Use;

1.1.9 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 12.3;

1.1.10 "**Subprocessor**" means any person (including any third party, but excluding an employee of ExaVault) appointed by or on behalf of ExaVault to Process Personal Data on behalf of any Customer or its Affiliates in connection with the Terms of Use; and

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## 2. Processing of EU Customer Personal Data

2.1 ExaVault shall not Process EU Customer Personal Data other than on the relevant Customer or its Affiliates' documented instructions unless Processing is required by Applicable Laws to which the relevant ExaVault is subject, in which case ExaVault shall to the extent permitted by Applicable Laws inform the relevant Customer or its Affiliates of that legal requirement before the relevant Processing of that Personal Data.

2.2 Each Customer or its Affiliates:

2.2.1 instructs ExaVault (and authorizes ExaVault to instruct each Subprocessor) to:

2.2.1.1 Process EU Customer Personal Data; and

2.2.1.2 in particular, transfer EU Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Terms of Use; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 2.2.1 on behalf of each relevant Customer Affiliate.

2.2.3 The instruction set forth in section 2.2.1 pertains to any reasonable processing necessary to provide the services as described in the terms of service, and includes any instructions provided by Customer within the administered console of its ExaVault account.

2.3 *Authorization by Third Party Controller.* If the European Data Protection Legislation applies to the processing of EU Customer Personal Data and Customer is a processor, Customer warrants to ExaVault that Customer's instructions and actions with respect to that EU Customer Personal Data, including its appointment of ExaVault as another processor, have been authorized by the relevant controller.

2.4 *Description of processing*. Annex 1 to this Addendum sets out certain information regarding the ExaVault's Processing of the EU Customer Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other EU Data Protection Laws). Nothing in Annex 1 (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

## 3. ExaVault Personnel

ExaVault shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any ExaVault who may have access to the EU Customer Personal Data, ensuring in each case that access is limited to those individuals who need to know / access the relevant EU Customer Personal Data, as necessary for the purposes of the Terms of Use, and to comply with Applicable Laws in the context of that individual's duties to ExaVault, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

## 4. Security

4.1 ExaVault will provide the technological safeguards that are described in its Enterprise Grade Security Page.

4.2 Customer shall review the technological safeguards stated in 4.1 to ensure those safeguards constitute a level of security appropriate to the EU Customer Personal Data, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.3 In assessing the appropriate level of security, Customer shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

## 5. Subprocessing

5.1 Each Customer or its Affiliates authorises ExaVault to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Terms of Use.

5.2 ExaVault may continue to use those Subprocessors already engaged by ExaVault as at the date of this Addendum, subject to ExaVault in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Customer generally authorizes ExaVault to use any other third parties as subprocessors. ExaVault shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor, at https://www.exavault.com/compliance/gdpr/. If, within seven (7) of receipt of that notice, Customer notifies ExaVault in writing of any objections (on reasonable grounds) to the proposed appointment:

5.3.1 ExaVault shall not appoint (or disclose any EU Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Customer or its Affiliates and Customer has been provided with a reasonable written explanation of the steps taken.

5.3.2 If ExaVault determines it is not commercially reasonable to provide the Services without the use of the proposed Subprocessor, ExaVault may terminate the Customer Account with thirty (30) days' notice, and refund any payment made for services not fully rendered as of the termination date. Except as modified by this section such termination shall otherwise occur pursuant to Section 7 ("Term and Termination") of the Terms of Use.

5.4 With respect to each Subprocessor, ExaVault shall:

5.4.1 before the Subprocessor first Processes EU Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for EU Customer Personal Data required by the Terms of Use;

5.4.2 ensure that the arrangement between ExaVault and the relevant intermediate Subprocessor is governed by a written contract including terms which offer at least the same level of protection for EU Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between ExaVault and the Subprocessor, or before the Subprocessor first Processes EU Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Customer or its Affiliates(s) (and Customer shall procure that each Customer Affiliate party to any such Standard Contractual Clauses co- operates with their population and execution); and

5.4.4 provide to Customer for review such copies of the ExaVault's agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.

5.5 ExaVault shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of EU Customer Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of ExaVault.

5.6 To the extent the Standard Contractual Clauses are required by law to be entered into directly between Customer and the Subprocessor, then Customer authorizes ExaVault, as Customer's attorney-in-fact, to enter into the Standard Contractual Clauses on Customer's behalf with Subprocessor.

## 6. Data Subject Rights

6.1 Customer has reviewed the ExaVault technical and organizational measures to ensure they are appropriate to the categories of EU Customer Personal Data being stored by Customer using the Service. Because ExaVault does not know what categories of personal data will be stored using the service, this obligation must be fulfilled by Customer.

6.2 ExaVault shall:

6.2.1 promptly notify Customer if ExaVault receives a request from a Customer's Data Subject under any Data Protection Law in respect of EU Customer Personal Data; and

6.2.2 ensure that the ExaVault does not respond to that request except to acknowledge to the requestor that it has been received and forwarded to Customer as the relevant data controller; additional response shall only be on the documented instructions of Customer or the relevant Customer Affiliate or as required by Applicable Laws to which the ExaVault is subject, in which case ExaVault shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the ExaVault responds to the request.

## 7. Personal Data Breach

7.1 ExaVault shall notify Customer without undue delay upon ExaVault or any Subprocessor becoming aware of a Personal Data Breach affecting EU Customer Personal Data, providing Customer with sufficient information to allow each Customer or its Affiliates to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the EU Data Protection Laws.

7.2 ExaVault shall cooperate with Customer and each Customer or its Affiliates and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 Nothing in this section 7 alters the parties' financial responsibilities for the indemnities set forth in the Terms of Use; in particular Customer may be liable for ExaVault expenses in

mitigating a Personal Data Breach to the extent such breach was caused by an action or inaction by Customer.

## 8. Data Protection Impact Assessment and Prior Consultation

ExaVault shall provide reasonable assistance to each Customer or its Affiliates with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer or its Affiliates by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of EU Customer Personal Data by, and taking into account the nature of the Processing and information available to ExaVault. ExaVault may charge Customer a commercially reasonable fee for such assistance.

## 9. Deletion or return of EU Customer Personal Data

9.1 The date of the termination of the Customer Account pursuant to Section 7 ("Term and Termination") of the Terms of Use is the "**Cessation Date**". Subject to sections 9.2 and 9.3, ExaVault shall promptly and in any event within thirty (30) days after the Cessation Date, delete and procure the deletion of all copies of those EU Customer Personal Data.

9.2 Prior to the Cessation Date, Customer may use the ExaVault user interface to download all EU Customer Personal Data to Customer by secure file transfer.

9.3 ExaVault may retain EU Customer Personal Data to the extent required by Applicable Laws, and always provided that ExaVault shall ensure the confidentiality of all such EU Customer Personal Data, and shall ensure that such EU Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose. ExaVault may also retain information about the Customer, such as customer name, contact details, and purchase history, for purposes of communications that Customer has consented to, where such consent has not been withdrawn (e.g., direct marketing email list).

## 10. Audit rights

10.1 Subject to the limitations of sections 10.2 to 10.3, ExaVault shall make available to each Customer or its Affiliates on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Customer or its Affiliates or an auditor mandated by any Customer or its Affiliates in relation to the Processing of the EU Customer Personal Data by ExaVault.

10.2 Information and audit rights of the Customer or its Affiliates only arise under section 10.1 to the extent that the Terms of Use does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

10.3 Following receipt by ExaVault of a request from Customer for an audit or inspection pursuant to section 10.1, ExaVault and Customer will discuss and agree in advance on its reasonable start date, scope and duration of and security and confidentiality controls applicable to the audit/inspection.

10.4 ExaVault shall have the right to refuse access to any auditor, where ExaVault can specify a reasonable basis, such as affiliation with an ExaVault competitor or lack of proper qualification.

10.5 Customer shall pay the fees and expenses of the auditor/inspector. ExaVault may charge Customer a reasonable fee for ExaVault cooperation with the audit/inspection. ExaVault may require that the auditor sign any reasonable legal documentation to ensure the confidentiality of ExaVault trade secrets and confidential information.

10.6 ExaVault shall not be required to submit to more than one audit in any given calendar year, except for any additional audits or inspections which:

10.6.1 Customer or the relevant Customer Affiliate undertaking an audit reasonably and in good faith considers necessary because of genuine concerns as to ExaVault's compliance with this Addendum; or

10.6.2 A Customer or its Affiliates are required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of EU Data Protection Laws in any country or territory.

## 11. Restricted Transfers

11.1 Subject to section 11.3, each Customer or its Affiliates (as "data exporter") and ExaVault, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Customer or its Affiliates to that ExaVault.

11.2 The Standard Contractual Clauses shall come into effect under section 11.1 on the later of: 11.2.1 the data exporter becoming a party to them;

11.2.2 the data importer becoming a party to them; and

11.2.3 commencement of the relevant Restricted Transfer.

11.3 Section 11.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law. For the avoidance of doubt, the parties anticipate that the US-EU Privacy Shield program will provide adequate safeguards and transfers to the United States will not be Restricted Transfer.

11.4 *Transfers outside the US and EU*. The parties agree that ExaVault may use personnel or servers not located in the United States or the European Union. In the event that this is the case, the parties anticipate that the Standard Contractual Clauses will be the mechanism that prevents such Restricted Transfer to occur in compliance with Data Protection Law. In all cases ExaVault will ensure that such personnel are subject to appropriate confidentiality requirements, including standard contractual clauses similar to those in Annex 2 to this addendum, including any necessary changes to reflect changes in the law.

## 12. General Terms

12.1 *Governing law and jurisdiction*. Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

12.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Terms of Use with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Terms of Use.

12.1.3 If an obligation under the Standard Contractual Clauses, or other legal obligation, requires that the parties submit to a jurisdiction and/or use the laws of a nation within the EU, the parties choose the courts and law of Ireland.

12.2 *Priority of Documents*. Nothing in this Addendum reduces ExaVault's obligations under the Terms of Use in relation to the protection of Personal Data or permits ExaVault to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Terms of Use. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. Subject to section 12.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Terms of Use and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

12.3 *Good Faith Negotiations To Revise, If Required By Law*. If any variations to this Addendum, (including any Standard Contractual Clauses entered into under section 11.1), as it applies to Restricted Transfers which are subject to a particular Data Protection Law, are required as a result of any change in, or decision of a competent authority under, that Data Protection Law the Parties agree to review each other's proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified for compliance with the Data Protection Law.

12.4 *Severance*. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12.5 *Assumption of Obligations*. Either party may transfer and assign its benefits and obligations pursuant to this Addendum to a successor entity in a merger or acquisition, or to a third party in a sale of all or substantially all of the Party's assets.

# ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of EU Customer Personal Data as required by Article 28(3) GDPR.

*Subject matter and duration of the Processing of EU Customer Personal Data*

The subject matter and duration of the Processing of the EU Customer Personal Data are set out in the Terms of Use and this Addendum.

*The nature and purpose of the Processing of EU Customer Personal Data*

ExaVault provides data storage and file transfer services. ExaVault does not access, control, or review the data uploaded by Customer.

*The types of EU Customer Personal Data to be Processed*

ExaVault will store the data that is uploaded by customer to the Service. ExaVault will not access (except in response to a Customer request, e.g. a support request) or control the data uploaded.

*The categories of Data Subject to whom the EU Customer Personal Data relates*

Data relating to individuals provided to ExaVault via the Services, by (or at the direction of) Customer or by Customer's end users.

*The obligations and rights of Customer and Customer Affiliates*

The obligations and rights of Customer and Customer Affiliates are set out in the Terms of Use and this Addendum.

# ANNEX 2: STANDARD CONTRACTUAL CLAUSES

*These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the EU Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those EU Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the EU Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise)*

# 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

Name of the data exporting organisation: Customer, with customer details as provided at the time of signup for the Service.

Name of the data importing organisation: ExaVault, Inc., a California corporation Address: 3001 Bishop Dr, Suite 300, San Ramon, CA 94583
Tel.: +1 (510) 500-0245; e-mail: support@exavault.com

(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.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

## 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;

(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.

# 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-party beneficiary.

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 presented by 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 security measures;

(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**

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 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. 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 supervisory authority.

## 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 transferred anymore.

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.

# 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:

The "Customer" specified in the Terms of Use and the Data Processing Addendum.

## Data importer

The data importer is:

ExaVault, Inc., a California corporation.

## Data subjects

The personal data transferred concern the following categories of data subjects:
Data subjects include the individuals about whom data is provided to ExaVault via the Service.

## Categories of data

The personal data transferred concern the following categories of data:

Data uploaded by customer to the ExaVault service.

## Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

Customer's data.

## Processing operations

The personal data transferred will be subject to the following basic processing activities:

Data storage and transfer. ExaVault does not access, control, or review the data uploaded by Customer

# APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The technical and organisational security measures implemented by the data importer in accordance with

Clauses 4(d) and 5(c) are located at
https://www.exavault.com/why-exavault/enterprise-security/