DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Terms of Service or other written or electronic agreement (the "Agreement") between VividCortex, Inc. ("VividCortex") and _____ ("Customer") for the purchase of VividCortex' subscription service (the "Services") to reflect the parties' agreement with regard to the Processing of Personal Data.

In the course of providing the Services to Customer pursuant to the Agreement, VividCortex may Process Personal Data on behalf of Customer. The parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent VividCortex processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Customer entity signing this DPA has executed an Order Form with VividCortex pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor any other agreement directly with VividCortex, but is instead a customer indirectly via an authorized reseller of the Services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

Except where otherwise expressly agreed by the parties in writing, this DPA shall not replace any additional rights relating to Processing of Customer Data previously negotiated by Customer in the Agreement (including any existing data processing addendum to the Agreement).

HOW TO EXECUTE THIS DPA:

This DPA consists of two parts: the main body of the DPA, and Schedule 1.

1. To complete this DPA, Customer must:
    a. Complete the information and sign on Page 5.
    b. Complete the information regarding the data exporter in Schedule 1.
    c. Complete the information in the signature box and in Schedule 1.
2. Submit the completed and signed DPA to VividCortex.
3. VividCortex will sign and return the DPA to the Customer, at which time this DPA will become legally binding.

DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and VividCortex, but has not signed its own Order Form with VividCortex and is not a "Customer" as defined under the Agreement.

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

"Customer Data" means what is defined in the Agreement as "Customer Data".

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

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

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable person.

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

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

"Security Practices Document" means the Information Security Practices Document, as updated from time to time, and accessible via the link in Appendix 2 to Schedule 1.

"Standard Contractual Clauses" means the agreement executed by and between Customer and VividCortex and attached hereto as Schedule 1 pursuant to the European Commission's decision (C(2010)593) of 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 data protection.

"Sub-processor" means any Processor engaged by VividCortex.

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

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, VividCortex is the Processor and that VividCortex will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 VividCortex Processing of Personal Data. VividCortex shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Requests. VividCortex shall, to the extent legally permitted, promptly notify Customer if VividCortex receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, VividCortex shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, VividCortex shall upon

Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent VividCortex is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from VividCortex's provision of such assistance.

4. VIVIDCORTEX PERSONNEL

4.1 Confidentiality. VividCortex 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 on their responsibilities and have executed written confidentiality agreements. VividCortex shall ensure that such confidentiality obligations survive the termination of the personnel engagement with VividCortex.

4.2 Reliability. VividCortex shall take commercially reasonable steps to ensure the reliability of any VividCortex personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. VividCortex shall ensure that VividCortex's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Data Protection Officer. VividCortex has appointed a data protection officer, who may be reached at security@vividcortex.com.

5. SUBPROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that VividCortex may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services VividCortex has retained them to provide, and they are prohibited from using Personal Data for any other purpose.

5.2 List of Current Sub-processors and Notification of New Sub-processors. VividCortex shall make available to Customer the current list of its Sub-processors. Such Sub-processor list shall include the identities of those Sub-processors and their country of location ("Sub-processor List"). Customer may view the list https://www.vividcortex.com/product/security/gdprlist. Customer will receive notifications of new Sub-processors for the Services which are provided to Customer by VividCortex, and if Customer subscribes, VividCortex shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3 Objection Right for New Sub-processors. Customer may object to VividCortex' use of a new Sub-processor by notifying VividCortex promptly in writing within ten (10) business days after receipt of VividCortex' notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, VividCortex will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If VividCortex is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by VividCortex without the use of the objected-to new Sub-processor by providing written notice to VividCortex. VividCortex will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

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

6. SECURITY

6.1 Controls for the Protection of Customer Data. VividCortex shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in VividCortex' Security Practice Document. VividCortex regularly monitors compliance with these measures. VividCortex will not materially decrease the overall security of the Services during a subscription term.

6.2 Certifications. VividCortex has obtained the third-party certifications and audits as described in VividCortex' Security Practices Document. Upon Customer's written request at reasonable intervals, VividCortex shall provide a copy of its then most recent third-party audits or certifications, as applicable, or any summaries thereof, that VividCortex generally makes available to its customers at the time of such request

7. SECURITY BREACH INCIDENT MANAGEMENT AND NOTIFICATION

7.1 Security Breach. VividCortex maintains security incident management policies and procedures and shall, notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by VividCortex or its Sub-processors of which VividCortex becomes aware (a "**Security Breach**"). VividCortex shall make reasonable efforts to identify the cause of such Security Breach and take those steps as VividCortex deems necessary and reasonable in order to remediate the cause of such a Security Breach to the extent the remediation is within VividCortex' reasonable control. The obligations herein shall not

apply to incidents that are caused by Customer or Customer's Users.

7.2 Unsuccessful Security Breach. Customer agrees that:

(i) An unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Customer's Personal Data or to any of VividCortex' equipment or facilities storing Customer's Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

(ii) VividCortex' obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by VividCortex of any fault or liability with respect to the Security Breach.

8. RETURN AND DELETION OF CUSTOMER DATA

VividCortex shall return Customer Data to Customer and/or to the extent allowed by applicable law, delete Customer Data in accordance with VividCortex' procedures and Data Protection Laws and/or consistent with the terms of the Agreement.

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the applicable limitation of liability section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA together.

10. EUROPEAN SPECIFIC PROVISIONS

10.1 GDPR. With effect from 25 May 2018, VividCortex will Process Personal Data in accordance with the GDPR requirements directly applicable to VividCortex' provision of its Services.

10.2 Standard Contractual Clauses. The Standard Contractual Clauses in Attachment 1 and the additional terms in this Section 10 will apply to the Processing of Personal Data by VividCortex in the course of providing the Services.

i. The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) or Switzerland to outside the EEA or Switzerland, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive or Swiss Federal Data Protection Act, as applicable), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors.

ii. The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an order. For the purpose of the Standard Contractual Clauses and this Section 10, the Customer and its Affiliates shall be deemed to be "Data Exporters".

10.3 Complete Agreement. This DPA and the Agreement are Data Exporter's complete and final instructions to Data Importer for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Data Exporter to Process Personal Data: (a) in accordance with the Agreement and applicable orders; and (b) to comply with other reasonable instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Agreement.

10.4 Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand; and, that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.

10.5 Data Protection Impact Assessment. With effect from 25 May 2018, upon Customer's request, VividCortex shall 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 Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to VividCortex. VividCortex shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 10.5, to the extent required under the GDPR.

10.6 Audit. The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Data Exporter's request, and subject to the confidentiality obligations set forth in the Agreement, Data Importer shall, within a reasonable period following such request, make available to Data Exporter (or Data Exporter's independent, third- party auditor that is not a competitor of VividCortex) information regarding VividCortex' compliance with the obligations set forth in this DPA in the form of the third- party certifications and audits it carries out as described in the Agreement and/or the Security Practices Document to the extent VividCortex makes them generally available to its customers. Customer may contact Data Importer in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Data Importer for any time expended for any such on-site audit at VividCortex' then-current

professional services rates, which shall be made available to Data Exporter upon request. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Data Exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Data Importer. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit.

10.7 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request

10.8 Order of Precedence. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail, provided, however, in the event that Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (1) VividCortex' EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications and (2) the Standard Contractual Clauses.

11. List of Schedules. The following is a list of the Schedules attached to this DPA:

- Schedule 1: Standard Contractual Clauses

12. Legal Effect. This DPA shall only become legally binding between Customer and VividCortex when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed. If this document has been electronically signed by either party such signature will have the same legal affect as a handwritten signature.

IN WITNESS WHEREOF, the parties hereto have signed this Agreement.

VividCortex, Inc.	**Customer**: _____
By:_____	By: _____
Name:_____	Name: _____
Title:_____	Title: _____
Date: _____	Date: _____

SCHEDULE 1 - STANDARD CONTRACTUAL CLAUSES

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:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: VividCortex, Inc.

Address: 300 Preston Ave, Charlottesville, VA 22902

Tel.: + 1-877-738-2863; e-mail: privacy@vividcortex.com

Other information needed to identify the organisation: Not applicable

(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;

(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

- 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.

- 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.

On behalf of the data exporter:

Name (written out in full): Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……. (stamp of organisation)

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):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of one or more Order Form(s).

Data importer

The data importer is:

VividCortex is a provider of Database Monitoring Applications and Services, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Nature of data

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

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following:

- To assist in the discovering, analyzing, and resolving production application database query issues. The issues could result in poor performance, deadlock, resources over utilization, etc. Resolving them in an expeditious manner improves production performance and reliability.

Categories of data

The personal data transferred concern the following categories of data:

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Samples of text taken from database 'queries'. Sample text data may include the following personally identifiable data of the Data Subject:

- Phone number
- Email address
- IP Address
- Browser Cookies
- Session IDs
- Merchant Account IDs

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- May contain any business or sensitive data contained within the database if not filtered by the customer.

Processing operations

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

- The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER

Name:……..…

Authorised Signature ……

DATA IMPORTER

Name:……..…

Authorised Signature ……

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):

TECHNICAL AND ORGANIZATIONAL MEASURES

Taking into account the state of the art, the costs of implementation and the nature, scope, content and purposes of the Processing, VividCortex agrees to implement the following technical and organizational measures:

SECURITY & PRIVACY DOCUMENTATION

Commitment to Security & Privacy

VividCortex is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our suite of products and services, including data submitted by customers to our online service ("Customer Data").

Covered Services

This documentation describes the security-related and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the VividCortex services.

Data Processing

VividCortex has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by VividCortex and its sub-processors.

Information Security Management Program ("ISMP")

VividCortex maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of VividCortex's business; (b) the amount of resources available to VividCortex; (c) the type of information that VividCortex will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

ISMP is designed to:

- Protect the integrity, availability, and prevent the unauthorized disclosure by VividCortex or its agents, of Customer Data in VividCortex's possession or control;
- Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by VividCortex or its agents;
- Protect against unauthorized access, use, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard information as set forth in any local, state or federal regulations by which VividCortex may be regulated.

1) Security Standards. VividCortex's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:

a) Internal risk assessments;

b) ISO 27001, 27002 and 27018 standards;
c) NIST guidance; and
d) SOC2 (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report").

2) Security Audit Report. VividCortex provides its customers, upon their request, with a copy of VividCortex's then-current Audit Report, including information as to whether the Security Audit revealed any material findings in the Service; and if so, the nature of each finding discovered.

3) Assigned Security Responsibility. VividCortex assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:
a) Designating a security official with overall responsibility; and
b) Defining security roles and responsibilities for individuals with security responsibilities.

4) Relationship with Sub-processors. VividCortex conducts reasonable due diligence and security assessments of sub-processors engaged by VividCortex in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.

5) Background Check. VividCortex performs background checks on any employees and contractors who are to perform material aspects of the Service or have access to Customer Data.

6) Security Policy, Confidentiality. VividCortex requires all personnel to acknowledge in writing, at the time of hire, that they will comply with the ISMP and protect all Customer Data at all times.

7) Security Awareness and Training. VividCortex has mandatory security awareness and training programs for all VividCortex personnel that address their implementation of and compliance with the ISMP.

8) Disciplinary Policy and Process. VividCortex maintains a disciplinary policy and process in the event VividCortex personnel violate the ISMP.

9) Access Controls. VividCortex has in place policies, procedures, and logical controls that are designed:
a) Controls to ensure that only those VividCortex personnel with an actual need-to-know will have access to any Customer Data;
b) Controls to ensure that all VividCortex personnel who are granted access to any Customer
c) Data are based on least-privilege principles;
d) Password and other strong authentication controls that are made available to VividCortex customers for access into products.
e) Periodic (no less than quarterly) access reviews to ensure that only those VividCortex personnel with access to Customer Data still require it.

10) Physical and Environmental Security. VividCortex contracts with AWS who maintains controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly-authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes.

11) Data Encryption.
a) Encryption of Transmitted Data: VividCortex uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the customer browser(s), and between its servers and customer's server(s).
b) Encryption of At-Rest Data: VividCortex uses Internet-industry standard secure encryption methods designed to protect stored Customer Data at rest. Such information is stored on server(s) that are not accessible from the Internet.
c) Encryption of Backups: All sensitive data within backups are encrypted.

12) Disaster Recovery. VividCortex maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:
a) Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;
b) Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested no less than annually;
c) RPO / RTO: Recovery Point Objective is no more than 24 hours and Recovery Time Objective is no more than 48 hours;
d) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

13) Secure Development Practices. VividCortex adheres to the following development controls:
a) Development Policies: VividCortex follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10 and SANS Top 20 Critical Security Controls; and
b) Training: VividCortex provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training by the security team regarding VividCortex's secure application development practices.

14) Data Integrity and Management. VividCortex maintains policies that ensure the following:
a) Segregation of Data: The Service includes logical controls, including encryption, to segregate each customer's Customer Data from that of other customers; and
b) Back Up/Archival: VividCortex performs full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

15) Vulnerability Management. VividCortex maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:
a) Scans: VividCortex performs daily, monthly and quarterly vulnerability scans on its environments. Vulnerabilities are remediated on a risk basis. VividCortex installs all medium, high, and critical security patches for all components in its production environment as soon as commercially possible;

b) External Application Vulnerability Assessment: VividCortex engages third parties to perform network vulnerability assessments and penetration testing on an annual basis. Reports from VividCortex's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request.

c) Vulnerabilities are remediated on a risk basis. VividCortex installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

16) Change and Configuration Management. VividCortex maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

a) A process for documenting, testing and approving the promotion of changes into production;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c) A process for VividCortex to perform security assessments of changes into production.

17) Secure Deletion. VividCortex maintains policies and procedures regarding the deletion of Customer Data taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted using secure deletion methods.

18) Intrusion Detection. VividCortex monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. VividCortex may analyze data collected by users' web browsers for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

19) Incident Management. VividCortex has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by VividCortex or its agents of which VividCortex becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in VividCortex's security incident response plan include:

a) Roles and responsibilities: formation of an internal incident response team with a response leader;

b) Investigation: assessing the risk the incident poses and determining who may be affected;

c) Communication: internal reporting as well as a notification process in the event of a Security Breach;

d) Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

e) Audit: conducting and documenting a root cause analysis and remediation plan.

20) VividCortex publishes system status information. VividCortex uses https://vividcortex.statuspage.io/ for service updates. VividCortex typically notifies customers of significant system incidents by subscription email to the listed contact, and for availability incidents the continue, may invite impacted customers to join a conference call about the incident and VividCortex's response.

21) Security Breach Management.

a) Notification: In the event of a Security Breach, VividCortex notifies impacted customers of such Security Breach. VividCortex cooperates with an impacted customer's reasonable request for information regarding such Security Breach, and VividCortex provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.

b) Remediation: In the event of a Security Breach, VividCortex, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

22) Logs. VividCortex provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. VividCortex (i) backs-up logs on a daily basis, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with VividCortex's data retention policy.

DATA EXPORTER

Name:……..…

Authorised Signature ……

DATA IMPORTER

Name:……..…

Authorised Signature ……