Data Processing Addendum

Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2010/87/EU - Standard Contractual Clauses (Processors) and including other applicable privacy and data security laws and regulations.

This Data Processing Addendum ("DPA") is entered into between Duboce Labs, Inc. ("pganalyze") and Customer (collectively, the "Parties") and forms part of the Master Subscription Services Agreement (or other such titled written or electronic agreement addressing the same subject matter) ("Agreement") between pganalyze and Customer for the subscription and software services ("Services") provided to Customer through the Agreement.

The Parties are entering into this DPA to ensure that the processing of Personal Data provided to pganalyze is done in a manner compliant with Data Protection Laws and Regulations and its requirements regarding the collection, use and retention of Personal Data of Data Subjects.

1. Definitions.

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement. "Control," for purposes of this definition, means direct or indirect ownership or control of 50% or more of the voting interests of the subject entity.

1.2. "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to Data Protection Laws and Regulations, and (b) is permitted to use the Services pursuant to the Agreement between Customer and pganalyze, but has not signed the Agreement or its own applicable Order Form with pganalyze and is not a "Customer" as defined under the Agreement.

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

1.4. "**Customer Data**" means all electronic data submitted by or on behalf of Customer, or an Authorized Affiliate, to the Services.

1.5. "**Data Protection Laws and Regulations**" means all laws and regulations, including, without limitation, the California Consumer Privacy Act (CPPA) and laws and regulations of the European Union (including GDPR), the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

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

1.7. "**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).

1.8. "**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data (as defined in the Agreement).

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

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

1.11. "**Security Documentation**" means the security documentation set forth in **Appendix 2**, as may be updated periodically, and incorporated within the Agreement.

1.12. "**pganalyze**" means Duboce Labs, Inc., a company incorporated in Delaware and its primary address as 2201 12th Ave, San Francisco, CA 94116, USA, or an Affiliate of pganalyze, as applicable.

1.13. "**pganalyze Group**" means pganalyze and its Affiliates engaged in the Processing of Personal Data.

1.14. "**Standard Contractual Clauses**" means the agreement executed by and between Customer and pganalyze, attached and included herein, 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, as may be amended, updated, or otherwise replaced from time to time.

1.15. "**Sub-processor**" means any Processor engaged by pganalyze or a member of the pganalyze Group.

1.16. "**Supervisory Authority**" means an independent public authority which is established by either: (a) applicable Data Protection Laws and Regulations; or (b), a member state of the European Union or European Economic Area, Switzerland, or United Kingdom pursuant to the GDPR.

2. Parties Respective Roles Regarding Personal Data. The parties agree that with regard to the Processing of Personal Data for Hosted Services as defined in the Master Subscription Services Agreement, Customer is the Controller, pganalyze is the Processor, and that pganalyze or members of the pganalyze Group will engage Sub-processors pursuant to and subject the requirements of this DPA.

3. Customer Responsibilities. 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 and legality of Personal Data provided by Customer to pganalyze and the means by which Customer acquired such Personal Data.

4. Processing Purposes. pganalyze shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions solely for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Authorized Users in their use of the Services; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. pganalyze shall promptly notify the Customer if, in its reasonable opinion, the Customer's instruction would not comply with the EU Data Protection Laws and Regulations, and pganalyze shall not be required to comply with or observe Customer's instructions if such instructions pertain to Personal Data of an EU resident and would violate the GDPR or other EU law or EU member state data protection provisions.

5. Scope of Processing. The subject-matter of Processing of Personal Data by pganalyze is the provision of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in **Appendix 1** to this DPA.

6. Data Subject Requests. To the extent legally permitted, pganalyze shall promptly notify Customer if pganalyze receives a request from a Data Subject to exercise the Data Subject's rights under applicable Data Protection Laws and Regulations ("Data Subject Request"). Factoring into account the nature of the Processing, pganalyze shall assist Customer by appropriate organizational and technical 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, pganalyze shall, upon Customer's request, provide commercially-reasonable efforts to assist Customer in responding to a Data Subject Request, to the extent that pganalyze is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. In addition, pganalyze will, to the extent applicable or as otherwise required by applicable Data Protection Laws and Regulations, make available technical options within pganalyze's platform, to enable self-help response to Data Subject Requests.

7. pganalyze Personnel.

7.1. Confidentiality. pganalyze shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have committed themselves to confidentiality through executed written confidentiality agreements. pganalyze shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

7.2. Reliability. pganalyze shall take commercially-reasonable steps to ensure the reliability of any pganalyze personnel engaged in the Processing of Personal Data

7.3. Limited Access. pganalyze shall ensure that pganalyze's access to Personal Data is limited to those personnel assisting in the provision of the Services in accordance with the Agreement.

7.4. Data Protection Officer. pganalyze has appointed a data protection officer. The appointed person may be reached at privacy@pganalyze.com.

8. List of Sub-processors. Subject to the terms and conditions set forth in the Agreement, Customer acknowledges and agrees that pganalyze may engage the use of third party Sub-processors in connection with the performance of Services under the Agreement. pganalyze shall enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor. pganalyze shall make available to Customer a list of its then-current Sub-processors. Pganalyze shall give Customer prior written notice of the retention of any new Sub-processor. Customer shall notify pganalyze of an objection to a newly retained Sub-processor promptly in writing within ten (10) business days after receipt of pganalyze's notice. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, pganalyze will use reasonable efforts to make available to Customer a change in the Services and/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 pganalyze is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may (a) deactivate that portion of the Services, or (b) if deactivation is not feasible, terminate the Agreement and/or applicable Order Form(s) with respect only to those aspects of the Services which cannot be provided by pganalyze without the use of the objected-to new Sub-processor by providing written notice to pganalyze. pganalyze will refund Customer a pro-rata portion of any prepaid fees covering the remainder of the term of the affected Services following the effective date of termination. The parties agree that the copies of the Sub-processor agreements that must be provided by pganalyze to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, redacted by pganalyze beforehand; and, that such copies will be provided by pganalyze, in a manner to be determined in its discretion, only upon request by Customer. The parties agree and acknowledge that to the extent required by applicable law they shall enter into any amending or superseding version of the Standard Contractual Clauses or any other similar agreement approved by the European Commission to ensure an adequate level of protection with respect to the privacy rights of Data Subjects.

9. Liability for Sub-processors. pganalyze shall be liable for the acts and omissions of its Sub-processors to the same extent pganalyze 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.

10. Security Measures. pganalyze shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data), confidentiality, and integrity of Customer Data, as set forth in pganalyze's applicable Security Documentation. pganalyze shall regularly assess, and evaluate the effectiveness and its compliance with these measures. pganalyze will not materially decrease the overall security of the Services during the term of the Agreement.

11. Third-Party Certifications and Audit Results. Upon Customer's written request at reasonable intervals, and subject to the execution of non-disclosure and confidentiality terms if not otherwise set forth in the Agreement, pganalyze shall make available to Customer a copy of pganalyze's then most recent third-party certifications or audit results, as applicable to demonstrate compliance with this DPA.

12. Notifications Regarding Customer Data. pganalyze has in place reasonable and appropriate security incident management policies and procedures, as specified in the Agreement and related Security Documentation and shall notify Customer without undue delay (but in no event later than any periods required by applicable Data Protection Laws and Regulations or described in the Agreement) after becoming aware of the unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data, including Personal Data, transmitted, stored or otherwise Processed by pganalyze or its Sub-processors of which pganalyze becomes aware (hereinafter, a "Customer Data Incident") and shall assist Customer in ensuring compliance with its obligations under applicable Data Protection Laws and Regulations. pganalyze shall make reasonable efforts to identify the cause of such Customer Data Incident, and take steps as pganalyze deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident, to the extent that the remediation is within pganalyze's reasonable control.

13. Return of Customer Data. pganalyze shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and time periods specified in the Agreement and related Security Documentation, unless the retention of the data is requested from pganalyze according to mandatory statutory laws.

14. Authorized Affiliates. The parties agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between pganalyze and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.

14.1. Communications. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with pganalyze under this DPA, and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

14.2. Exercise of Rights. Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against pganalyze directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

16. Processing and Recordkeeping. Pganalyze will Process Personal Data in accordance with the GDPR requirements and Data Protection Laws and Regulations applicable to pganalyze's provision of the Services. Pganalyze shall maintain a record of all categories of processing activities carried out on behalf of Customer as required by applicable Data Protection Laws and Regulations.

17. Data Protection Impact Assessment. Upon Customer's request, pganalyze 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 pganalyze. pganalyze shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks to the extent required under the GDPR.

18. Standard Contractual Clauses. If any transfer of Personal Data between pganalyze and Customer (or pganalyze and its Sub-processors) requires or otherwise utilizes Standard Contractual Clauses in order to comply with applicable Data Protection Laws and Regulations, the parties hereby execute such Standard Contractual Clauses attached hereto. The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed the Agreement and/or applicable Order Form(s) for the Services. For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters."

18.1. Essential Equivalence. In the event either Party believes, in its reasonable discretion, that it is unable to comply with the requirements set forth in the Standard Contractual Clauses (as may be supplemented in accordance with its terms) such Party shall notify the other Party of such determination and the other Party may, if it agrees with such determination and the Parties

cannot reasonably supplement the Standard Contractual Clauses with additional terms and conditions that would provide the required level of protection or adopt another cross-border data transfer mechanism that will provide the required level of protection, suspend any further transfers of Personal Data or terminate the Agreement.

18.2. Access Requests and Compelled Disclosures. pganalyze shall notify Customer of any requests to access or otherwise disclose Personal Data pursuant to applicable federal, state, or local law, regulation, or valid order issued by a court or governmental agency or authority of competent jurisdiction (a "Legal Order") will be subject to the terms of this paragraph. Prior to making such a disclosure, pganalyze shall, to the extent permitted under the Legal Order, provide Customer with: (a) prompt written notice of such requirement so that Customer may seek, at its sole cost and expense, to challenge such access or disclosure or to obtain a protective order or other remedy; and (b) reasonable assistance, at Customer's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If, after providing such notice and assistance as required herein, pganalyze remains subject to a Legal Order to disclose any Personal Data, pganalyze shall disclose no more than the portion of Personal Data which, on the advice of pganalyze's legal counsel, such Legal Order specifically requires pganalyze to disclose.

19. Customer's Processing Instructions. This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to pganalyze 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 instructions set forth in Section 4 of this DPA are deemed Customer's instructions to pganalyze for the Processing of Personal Data.

20. Data Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by pganalyze to Customer only upon Customer's request.

21. Order of Precedence. This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

Each Party has executed this DPA by their authorized representatives:

pganalyze:	**Customer: [Via Online Acceptance]**
By: DocuSigned by: Lukas Fittl CCE2740F9E6E44E...	By:
Name: Lukas Fittl	Name:

Title: CEO
Date: 1/29/2021

Title:
Date:

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 organization:.....

Address:.....

Tel.:..... ; fax:..... ; e-mail:.....

Other information needed to identify the organization:

……

(the data **exporter**)

And

Name of the data importing organization:

Duboce Labs, Inc.

2201 12th Ave

San Francisco, CA 94116

E-mail: privacy@pganalyze.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.

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 organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 organizational 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, unauthorized 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 organizational 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 unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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.

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…….

On behalf of the data importer:
Name (written out in full): Lukas Fittl
Position: CEO
Address: Duboce Labs, Inc., 2201 12th Ave, San Francisco, CA 94116

Other information necessary in order for the contract to be binding (if any):

Signature

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.

Details about data processing

1. Data to be processed/Data affected for the PostgreSQL Performance Monitoring services pursuant to the Master Subscription Services Agreement:

a. Categories of data subjects:

☐ Candidates
☒ Customers
☒ Employees
☐ Interested Parties
☐ Subscribers
☐ Suppliers
☐ Others:

b. Affected types or categories of personal data:

☒ Personal master data, e.g. first name, second name and user name.
☒ Contact details, e.g. telephone, e-mail.
☒ Contract master data e.g. contractual relationship, interest in products or contracts.
☒ Contract invoicing and payment data (e.g. bank account).
☒ Other personal data, especially database statistics information uploaded to pganalyze's servers, which may contain or reference other kinds of personal data.

c. Sensitive Data/Special categories of Data within the meaning of Art. 9 of the EU General Data Protection Regulation (GDPR) (must be specified in detail here):

☐ Health data
☐ Genetic data
☐ Biometric data for the unequivocal identification of a natural person
☐ Data revealing racial or ethnic origin
☐ Political opinions
☐ Religious or philosophical beliefs
☐ Trade union membership
☐ Data concerning a natural person's sex life or sexual orientation

d. Access to personal data

(Please describe how the Processor receives the personal data or gets access to it, e.g., transfer via a secure connection, access to target system/target application, data collection via special interfaces, etc.)

☒ The Controller provides the Processor with the Data, enables the Processor to access the Data, or allows the Processor to collect the Data as described below:
According to the Master Subscription Services Agreement.

and/or:

☒ Services in the area of maintenance/remote maintenance/IT fault analysis shall be provided. The possibility that the Processor may get access to the Data cannot be excluded in the context of performance of these services.

2. Services, purpose of the Processing: According to the Master Subscription Services Agreement

3. Processing location: All Customer's data that is processed through pganalyze's Hosted Services will be hosted permanently at data centers run by Amazon Web Services, Inc.

DATA EXPORTER
Name: Customer identified in connection with pganalyze online Terms of Service

……

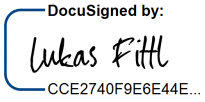
Authorized Signature:

Online acceptance of Terms of Service

DATA IMPORTER
Name:

Lukas Fittl

Authorized Signature:



Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. Acceptance of pganalyze's online Terms of Service shall constitute execution by Customer.
Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data contained in Customer Data, as described in the Security Documentation. Data Importer will not materially decrease the overall security of the Services during the term of the Agreement.

Security Documentation

In order to protect the data of our customers and their customers, pganalyze follows industry standard practices, as outlined in our policy documents. Policy details are available by emailing security@pganalyze.com.

Data Transit Security

pganalyze uses encryption both in transit and at rest.

Annex 4

Information about Subprocessors

Within the scope of Master Subscription Services Agreement, the Processor intends to deploy the following Subprocessors for the following services/at the following Processing locations:

#	Entity Name	Processing Activities	Location
1	Sentry.io	Application monitoring provider	United States
2	Hubspot	Customer relations management	United States
3	Google Marketing Platform	Analytics, Ad Conversion & Retargeting	United States
4	Segment	Analytics	United States
5	Customer.io	Transactional mail services provider	United States
6	Amazon AWS	Data hosting	United States
7	Google Apps	Internal company infrastructure	United States
8	Zendesk	Customer support ticketing system	United States
9	Stripe	Payment provider	United States
10	Skylight.io	Application monitoring provider	United States
11	Cloudflare	Content delivery network	United States
12	Twitter	Ad Conversion & Retargeting	United States
13	Perfect Audience	Ad Conversion & Retargeting	United States
14	Heroku	Data hosting	United States

California Data Processing Addendum

This California Data Processing Addendum ("Addendum") forms a part of the Master Subscription Services Agreement] by and between ("Customer") and Duboce Labs, Inc. ("pganalyze") effective as of the date of online acceptance of pganalyze's Terms of Service (the "Agreement"). The parties enter into this written amendment to the Agreement pursuant to the requirements of under California law, including the Consumer Privacy Act, California Civil Code Section 1798.100 ("CCPA") et seq., as amended generally from time to time and as amended by the California Privacy Rights Act effective January 1, 2023 ("CPRA") (collectively "Privacy Laws") as it pertains to pganalyze's processing of Personal Information of California residents and agree as follows:

1. **Definitions.** For purposes of this Addendum, capitalized terms not otherwise defined in the Agreement shall be defined pursuant to the Privacy Laws in effect at the time of pganalyze's processing of any Personal Information.

2. **Service Provider Designation.** The Parties agree and acknowledge that any disclosure of Consumers' Personal Information from Customer to pganalyze is necessary for the performance of the services provided pursuant to the Agreement, and not for monetary or other valuable consideration. pganalyze and Customer agree that pganalyze is (a) acting as a Service Provider as defined by the CCPA and (b) processing a Consumer's Personal Information on solely behalf of Customer and solely for the specific business purpose of performing the services set forth in the Agreement and not for its own commercial purposes or in a way that does not comply with applicable Privacy Laws.

3. **Scope of Processing Authority**. pganalyze shall not retain, use or disclose a Consumer's Personal Information for any purpose other than for the specific purpose of performing the services set forth in the Agreement.

4. **Prohibited Use.** pganalyze shall not Sell any Consumer Personal Information shared by Customer with pganalyze. pganalyze further agrees not to retain, use or disclose Consumer Personal Information obtained from Customer (i) outside the direct relationship between Customer and pganalyze, and (ii) for any purposes other than for providing the services specified in the Agreement.

5. **Deletion.** Upon Customer's written request, and subject to and in accordance with all applicable Privacy Laws, pganalyze agrees to promptly delete any and all Consumer Personal Information.

6. **CPRA.** pganalyze (a) shall comply with any and all applicable privacy laws and regulations relating to the Processing of Personal Information by or on behalf of Customer arising from or relating to the Services provided in connection with this Agreement, including, without limitation, applicable Privacy Laws, and (b) will provide the same level of privacy protection for Personal Information as is required by applicable Privacy Laws. Customer has the right to take reasonable and appropriate steps to ensure that pganalyze uses any Personal Information received from Customer in a manner consistent with pganalyze's obligations under Privacy Laws. To the extent pganalyze determines it can no longer meet its obligations under Privacy Laws applicable to Personal Information received from Customer, pganalyze will notify Customer of such determination and will reasonably cooperate with such Customer's reasonable and appropriate steps to stop and remediate any unauthorized use of such Personal Information.

pganalyze certifies that it understands the foregoing restrictions relating to Consumer Personal Information shared by Customer and shall comply with the obligations set forth herein and as otherwise required under applicable Privacy Laws.

pganalyze:

By: DocuSigned by: Lukas Fittl CCE2740F9E6E44E...
Name: Lukas Fittl
Title: CEO
Date: 1/29/2021

Customer: [Via Online Acceptance]

By:
Name:
Title:
Date: