Data Processing Agreement

This Data Processing Agreement (“DPA”) reflects the parties’ agreement with respect to the processing of Personal Data in connection with Customer orders and purchases of SENSEMETRICS, Inc. (“Company”) Products and Services.

If Customer is (a) located in a country or jurisdiction subject to the Data Protection Laws, and (b) transfers Personal Data to Company from such country or jurisdiction, this DPA is incorporated into the Customer Terms and Conditions (“Terms”) and supplements that agreement between Company and Customer.

In the event of any conflict or inconsistency between the DPA and Terms, the DPA shall prevail. The provisions of the DPA supersede any conflicting provisions of the Company’s Privacy Policy that otherwise may apply to the processing of Customer’s Personal Data.

1. DEFINITIONS

“Data Controller” means the Customer and its Permitted Affiliates.

“Data Processor” means the Company.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to each party as Data Controller (Customer) and Data Processor (Company) under the Agreement (as defined in Section 2.1), including without limitation European Data Protection Laws, and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated, or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

"Europe" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

"European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as these may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by the Data Controller to the Data Processor directing or authorizing it to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

"Permitted Affiliates" means any of Customer’s Affiliates (including its authorized users) that (i) are permitted to use the Platform pursuant to the Agreement but have not signed their own separate agreement with Company and are not a “Customer” as defined under the Agreement, (ii) qualify as a

Controller of Personal Data processed by Company, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer data and is protected similarly as personal data, personal information, or personally identifiable information under applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Company and/or its Sub-Processors in connection with the Agreement. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Sub-Processor” means any processor engaged by Company to assist in fulfilling its obligations under the Agreement. Sub-Processors may include third parties but will exclude any Company employee or consultant.

Note: capitalized terms used but not defined in this DPA shall have the definitions set forth in the separate Agreement between the parties.

2. PURPOSE, SCOPE, AND RESPONSIBILITIES

2.1 This DPA specifies the parties’ data protection obligations that arise from the Data Processor’s processing of Personal Data on behalf of the Data Controller under (a) the Quote and Terms, or (b) other written agreement between the parties (either [a] or [b], the “Agreement”). In the case of (a), this DPA applies pursuant to Section 27 of the Terms. In the case of (b), this DPA applies only if it is incorporated into the Agreement. When Customer renews an Agreement or purchases a new Software subscription, the then-current DPA will apply for that subscription term.

2.2 The Data Processor shall only process Personal Data in accordance with the terms of this DPA.

2.3 The Data Processor shall process Personal Data for the limited business purpose of performing its obligations under the Agreement.

2.4 The term of this DPA shall continue until the latter of the following: the termination of the Agreement, or the date on which the Data Processor ceases to process Personal Data for the Data Controller.

2.5 The Personal Data to be processed by the Data Processor concerns the categories of data, the categories of Data Subject, and the purposes of the processing set forth in Schedule A attached hereto.

2.6 With the exception of the data described in Schedule A, in no event will the data processed by the Data Processor include: (a) Personal Data as set out in Article 9 or 10 in Regulation 2016/679 of 27 April 2016; (b) Personal Data regarding finances; (c) Personal Data regarding criminal offenses, or (d) Personal Data regarding taxes, sick days, family relations, residential circumstances, car, personality tests, exams or CVs.

3. SENSEMETRICS PLATFORM

3.1 The Platform may enable the Data Controller to upload information without the Data Processor's participation or knowledge.

3.2 The Data Processor undertakes no responsibility for data uploaded by the Data Controller to the Platform.

3.3 To the extent that such upload of data constitutes processing of Personal Data, the Data Controller warrants: (a) the Data Controller has the relevant legal basis for possessing, transferring, and processing the Personal Data, including, if applicable, the relevant or required permissions from the Data Subject; (b) the transfer does not include sensitive categories of data; and (c) the Data Subject has been informed or will be informed before the transfer, or as soon as possible after, that its data could be transmitted to a third country not providing adequate protection within the meaning of the Data Protection Laws.

4. OBLIGATIONS OF THE DATA PROCESSOR

The Data Processor warrants that it will: (a) comply with the Data Protection Laws applicable to the Data Processor's obligations under this DPA, (b) process any Personal Data transferred to or collected by the Data Processor only as a "processor," as defined in the Data Protection Laws, on behalf of the Data Controller pursuant to Instructions, (c) implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the applicable Data Protection Laws and ensure the protection of the rights of the Data Subjects, (d) ensure that Sub-Processors process Personal Data in accordance with the DPA and Data Protection Laws, (e) taking into account the nature of the processing, assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Laws, (f) reasonably assist the Data Controller in ensuring compliance with the security requirements for Personal Data, (g) make available to the Data Controller all information reasonably necessary to demonstrate compliance with the DPA, and (h) reasonably allow for and contribute to audits conducted by the Data Controller at its expense or an auditor selected and paid for by the Data Controller.

5. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

5.1 The Data Processor will implement and maintain throughout the term of the DPA, and ensure or verify that its Sub-Processors implement and maintain through the term of the DPA, the appropriate technical and organizational security measures to protect Personal Data against accidental or unlawful destruction, loss, damage or alteration and against unauthorized disclosure, abuse or other processing in violation of the requirements of Data Protection Laws.

5.2 The Data Processor will ensure that it and verify that Sub-Processors involved in the processing of Personal Data at all times comply with the minimum data security requirements set forth in Schedule 2 attached hereto.

6. SENSEMETRICS PERSONNEL

6.2 The Data Processor will ensure that its personnel who are required to access Personal Data comply with the DPA and have confidentiality obligations similar to, but no less stringent than, those set forth in the Agreement.

6.2 The Data Processor will ensure that its personnel who have access to Personal Data are informed of the confidential nature of the Personal Data and the security procedures applicable to the processing of or access to the Personal Data.

6.3 The Data Processor will ensure that its personnel comply with the confidentiality obligations set forth in this Section Six following any expiration or termination of the Agreement and DPA.

7. ASSISTANCE TO THE DATA CONTROLLER

7.1 The Data Processor agrees to provide reasonable and timely assistance to Data Controller to enable Data Controller to respond to: (a) any request from a Data Subject to exercise any of its rights under the applicable Data Protection Laws (including its rights of access, correction, objection, and erasure, as applicable); and (b) any other correspondence, inquiry or complaint received from a Data Subject, regulator, or authorized third party in connection with the processing of the Personal Data. If any such request, correspondence, inquiry, or complaint is made directly to Data Processor, Data Processor shall promptly inform Data Controller and provide full details of the same.

7.2 The Data Processor will reasonably cooperate with Data Controller to enable Data Controller to conduct any data protection impact assessment that it is required to undertake under applicable Data Protection Laws.

8. SUB-PROCESSORS

8.1 Pursuant to this DPA, the Data Processor has the Data Controller's general authorization to engage Sub-Processors for the purpose of performing its obligations under the Agreement. The Sub-Processors approved by the Data Controller under this DPA are listed in Schedule 3 attached hereto.

8.2 The Data Processor will comply with the requirements set forth in Article 28(2) and (4) GDPR if it engages any Sub-Processors in addition to those listed in Schedule 3.

8.3 The Data Processor shall: (a) maintain an up-to-date list of its Sub-Processors and provide the list to the Data Controller upon request, (b) provide Data Controller with details of any change in Sub-Processors at least 30 days before any such change (except to the extent 30 days' notice is not possible due to an emergency) and notify the Data Controller of such change via the Data Processor's usual e-mail notification process, and (c) upon request, provide a copy of the data processing agreement(s) between the Data Processor and the Sub-Processors.

8.4 Upon receiving notice of a change to or addition of Sub-Processors, the Data Controller may object for justified reasons relating to the protection of Personal Data. All such objections shall be in writing and provided no later than 30 days after receiving notice. In the case of a justified objection, the Parties shall negotiate in good faith to find an alternative solution. If such alternative solution cannot be found and the Data Processor proceeds with such Sub-processor, the Data Controller may terminate the Agreement

upon providing 30 days written notice. Neither party shall be considered to have breached the Agreement due to such termination.

9. OBLIGATIONS OF THE DATA CONTROLLER

9.1 The Data Controller and the Data Processor will be separately responsible for complying with the Data Protection Laws as applicable to each.

9.2 The Data Controller shall be responsible for ensuring that the processing of Personal Data, which it instructs or authorizes the Data Processor to perform, has a legal basis under applicable Data Protection Laws.

9.3 The Data Controller will inform the Data Processor in writing without undue delay following the Data Controller's discovery of a failure to comply with Data Protection Laws with respect to processing of Personal Data in accordance with this DPA.

9.4 The Data Controller shall be responsible for providing accurate and relevant contact details after entering into the Agreement and thereafter to assist in Data Processor's notification obligations pursuant to this DPA.

9.5 The Data Controller shall indemnify and hold the Data Processor harmless from and against any Data Subject claims, losses, or damages arising from or related to Data Controller's failure to comply with applicable Data Protection Laws.

10. NOTIFICATION OF PERSONAL DATA BREACH

10.1 The Data Processor shall without undue delay, and no later than 48 hours, in writing, notify the Data Controller in case of any Personal Data Breach related to the DPA.

10.2 The notification under Section 10.1 above must, to the extent known or reasonably suspected: (a) describe the nature of the Personal Data Breach including (e.g., loss, theft, copying), the categories and approximate number of Data Subjects involved and the categories and approximate number of Personal Data records concerned, (b) communicate the name and contact details of the Data Processor officer handling the breach, (c) describe the likely or reasonably suspected consequences of the Personal Data Breach, and (d) describe the measures taken or proposed to be taken by the Data Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. ALLOCATIONS

11.1 The Data Processor shall carry all costs associated with compliance of this DPA in its capacity as Data Processor.

11.2 The Data Controller shall carry all costs associated with compliance of this DPA in its capacity as Data Controller.

11.3 The Data Controller may request that the Data Processor undertake tasks not required by this DPA, or which Data Processor is not obligated to perform pursuant to applicable Data Protection Laws. If Data Processor in its discretion agrees to such tasks, it shall be entitled to charge the Data Controller for the

additional resources, time, and material necessary to fulfill the requested task(s). In this event, (a) the Data Processor will notify the Data Controller in advance of such additional charges and, to the extent possible, provide the Data Controller with a Quote of the expected costs, and (b) if the Data Controller does not accept the Quote, the Data Processor may decline the request and/or terminate the Agreement by giving 30 days written notice. The Data Processor shall not be considered in breach of contract in this event.

12. DELETION AND RETURN OF PERSONAL DATA

12.1 Following the expiration or termination of the Agreement, the Data Processor shall (at Data Controller's election) destroy or return to Data Controller all Personal Data in its possession or control. The Data Processor reserves the right after 90 days to delete Personal Data from all locations when the Data Controller has not elected either option. This requirement shall not apply to the extent that Data Processor is required by the Agreement or applicable law to retain some or all of the Personal Data.

12.2 Upon the Data Controller's request, the Data Processor shall certify in writing the destruction of the Personal Data.

13. LIABILITY

Each party's liability for one or more breaches of this DPA shall be subject to the damages exclusions and liability limitations set forth in the Agreement. In no event shall either party's aggregate liability for a breach of this DPA exceed the liability limitations set forth in the Agreement. Neither party limits nor excludes any liability that cannot be limited or excluded under applicable law (such as for willful misconduct or fraud).

14. LEGAL VENUE AND APPLICABLE LAW

14.1 This DPA will be governed by and construed in accordance with the governing law section of the Agreement between the parties, unless mandated otherwise by applicable Data Protection Laws.

14.2 Exclusive venue for all claims or controversies arising from or relating to this DPA shall be (a) in the forum specified by the parties in their Agreement; or if no such forum is specified, then (b) in any court of competent jurisdiction located in the State of Delaware USA. With respect to (b), the parties hereby consent to jurisdiction in such courts.

15. PERSONAL DATA TRANSFERS

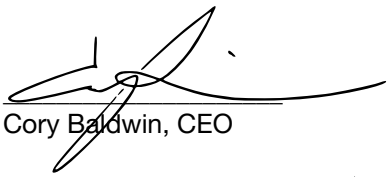
The parties to this DPA have a commercial relationship and performance of the Agreement between them requires the occasional and limited transfer of Personal Data from Customer and its employees to Company. In most cases, the transfer will occur no more than once for each Data Subject, and the Data Subject will be a Customer employee who has knowingly provided the Personal Data and consented to the transfer. Each such transfer of Personal Data will be limited to name and business contact information. Given the foregoing, the parties acknowledge that the Company's minimal processing of Personal Data pursuant to the Agreement and this DPA is for a lawful purpose, mutually beneficial, and serves each party's legitimate interests.

If additional, continuous, or more intensive transfers of Personal Data from Customer to Company become required for performance of the Agreement, the parties may amend this DPA by incorporating the then-current Standard Contractual Clauses applicable to Customer (as Data Controller and Exporter) and Company (as Data Processor and Importer). Any such amendment shall be in writing, may include additional commercial provisions, and must be signed by authorized representatives of each party.

16. SIGNATURES

The Customer's acceptance of the Quote and Terms, or execution of a separate agreement with Company that incorporates this DPA, shall constitute its signature.

For sensemetrics, Inc.



Cory Baldwin, CEO

Date: January 5, 2021

Attachments:

Schedule A – Processing Details
Schedule B – Security Measures
Schedule C – Authorized Sub-Processors

Schedule A: PROCESSING DETAILS

A. Nature and Purpose of Processing

Company will process Personal Data only as necessary to provide the Products and Services pursuant to the Agreement, as further specified in the Quote, and as further instructed by Customer in its use of the Platform. The content of this DPA reflects the limited amount of Personal Data the Data Processor will process for the Data Controller.

B. Duration of Processing

Subject to the "Deletion or Return of Personal Data" section of this DPA, Company will process Personal Data for the term of the Agreement, unless otherwise agreed in writing.

C. Categories of Data Subjects

Customer may submit Personal Data in the course of ordering Products and Services, or accessing and using the Platform, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Customer employees and Permitted Affiliates

D. Categories of Personal Data

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

- Contact Information (name, e-mail address, telephone number, address)
- Any other Personal Data that Customer and Permitted Affiliates upload to the Platform

E. Special Categories of Data

None. Customer shall not transfer, supply, or upload any special categories of data.

F. Processing Operations

Personal Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain, and administer the Products and Services purchased by Customer; and/or
- Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

G. Processing Location

750 B Street, Suite 1630, San Diego, California USA 92101

H. Processing Duration

Processing will commence on the effective date of the Agreement and will continue until the expiration or termination of same, or until Customer instructs Company to discontinue the processing of any Personal Data.

Schedule B: SECURITY MEASURES

1. Physical Access Controls

Data Processor shall take reasonable measures to prevent physical access, such as secured buildings, to prevent unauthorized persons from gaining access to Company computers or networks that process Personal Data.

2. System Access Controls

Data Processor shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or logging of access on several levels.

3. Data Access Controls

Data Processor shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of processing. The Data Processor shall take reasonable measures to implement an access policy under which access to its system environment, to Personal Data and other data by authorized personnel only.

4. Transmission Controls

Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport.

5. Input Controls

Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Personal Data has been entered into data processing systems, modified, or removed. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of the data supplier; and (ii) Personal Data integrated into Data Processor's systems is managed by secured file transfer from the Data Processor and Data Subject.

Schedule C: AUTHORIZED SUB-PROCESSORS

Vendor	Purpose	Entity Country	GDPR Resource
Zendesk	Support ticket management	USA	https://www.zendesk.com/company/customers-partners/eu-data-protection/
Salesforce	Sales and Lead management	USA	https://www.salesforce.com/gdpr/overview/
mixpanel	Platform analytics	USA	https://help.mixpanel.com/hc/en-us/articles/360000345423-GDPR-Compliance
NetSuite	Financial system	USA	https://www.oracle.com/applications/gdpr/
Mailchimp	Email marketing	USA	https://mailchimp.com/gdpr/
SaaSOptics	SaaS Subscription Management	USA	https://saasoptics.zendesk.com/hc/en-us/articles/360003671793-GDPR
Auth0	Identity Management	USA	https://auth0.com/docs/compliance/gdpr
Dialpad	Messaging and phone system	USA	https://storage.googleapis.com/dialpad/gdpr.pdf
Gusto	Human Resource system	USA	https://gusto.com/about/privacy
G Suite	Email Service	USA	https://cloud.google.com/security/gdpr/
Atlassian	Software Development tools	USA	https://www.atlassian.com/legal/data-processing-addendum
AWS	Data Hosting	USA	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Zapier	Platform Integrations	USA	https://cdn.zapier.com/storage/files/46ac3128100f09a5eeda6ceb7bdb61aa.pdf