Airbrake Global Data Processing Addendum (DPA)

This Data Processing Addendum **("DPA")**, forms part of the Subscription Agreement between Airbrake Technologies Holdings, Inc. ("**Airbrake**") and the undersigned customer of Airbrake ("**Customer**") for certain error monitoring, application optimization, and/or other services (collectively, the "**Service**") provided by Airbrake (the "**Main Agreement**"). All capitalized terms not defined herein shall have the meanings set forth in the Main Agreement. Each of Customer and Airbrake may be referred to herein as a "**party**" and together as the "**parties**."

The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by Data Protection Laws. This DPA is effective on the date that it has been duly executed by both parties, as evidenced by the date on the signature line of this DPA ("**Terms Effective Date**"), and supersedes and replaces any previously applicable terms relating to their subject matter (including any data processing amendment or data processing addendum relating to the Services. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail.

HOW THIS DPA APPLIES

This DPA is an addendum to and forms part of the Main Agreement. The Customer entity signing this DPA must be the same as the Customer entity party to the Main Agreement.

DATA PROCESSING TERMS

1. Definitions

1.1 The following definitions are used in this DPA:

a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with an entity signing the underlying Main Agreement.

b) "**Controller**" means the party that determines the purposes and means of the Processing of Personal Data, and includes a **"business"** as defined under the California Privacy Law.

c) "**Customer Group**" means Customer and any of its Affiliates to which Airbrake provides Services.

d) "**Customer Data**" means all Personal Data Processed by Airbrake on behalf of Customers to provide the Services under this DPA and the Main Agreement.

e) "**Data Protection Laws**" means all data protection and privacy laws and regulations applicable to the processing of Personal Data in connection with the Main Agreement, as they may be amended from time to time, in any jurisdiction, including but not limited to: (a) the European Economic Area and Switzerland, including (i) the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"), EU Member State laws supplementing the GDPR, and the Swiss Federal Act on Data Protection ("**Swiss DPA**"); (b) the UK Data Protection Act of 2018, and the UK GDPR (collectively, "**UK GDPR**"); and (c) the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq., (collectively referred to as the "**CCPA**" which, for clarity also includes the **CPRA**) and its implementing regulations (and, collectively, the "**California Privacy Law**"), as well as other applicable state, federal or international consumer privacy and data protection laws.

f) "**Data Subject**" means a natural person, and shall include "data subject" and "consumer" as those terms are defined under Data Protection Laws.

g) "**Deidentified Information**" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject.

h) **"EEA"** means the European Economic Area.

i) **"EEA Personal Data"** is Customer Data collected from data subjects when they are located in the EEA.

j) "**Personal Data**" has the meaning given by applicable Data Protection Laws and shall include information (regardless of the medium in which it is contained), whether alone or in combination with other available information that directly or indirectly identifies a Data Subject. Personal Data shall have the same meaning as "personal information" under California Privacy Laws.

k) "**Processing**" (including "**Process**" or "**Processed**") 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.

l) "**Processor**" means the party which Processes Personal Data on behalf of the Controller, and includes a "service provider" as defined under the California Privacy Law.

m) "**Regulator**" means any entity which has jurisdiction to enforce Airbrake's compliance with the Data Protection Laws.

n) "**Restricted Transfer**" means: (i) where the EU GDPR applies, transferring Personal Data collected from a Data Subject located in the EEA either directly or via onward transfer to a country that has not been issued an adequacy determination by the European Commission; (ii) where the UK GDPR applies, transferring, either directly or via onward transfer, Personal Data collected from a Data Subject located in the United Kingdom to or within any other country which is not subject based on adequacy regulations under Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 applies, transferring either directly or via onward transfer, Personal Data collected from a Data Subject located in Switzerland to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

o) "**Standard Contractual Clauses**" or "**SCC**" means: (i) where the EU GDPR applies, the clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for transferring personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council, available at, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN ("**EU SCC**"); (ii) where the UK GDPR applies, the International Data Transfer Agreement A1.0 issued by the ICO, available at: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf ("**UK IDTA**"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner, (in each case, as updated, amended or superseded from time to time)

p) "**Sub-Processor**" means any person or entity appointed by or on behalf of the Processor to Process Customer Data.

q) "**Swiss Personal Data**" means Customer Data collected from Data Subjects when they are located in Switzerland.

r) "**UK Personal Data**" means Customer Data collected from data subjects when they are located in the United Kingdom.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

2.1 The type of Customer Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Appendix 1.

2.2 Each party warrants in relation to Customer Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its Sub-Processors comply), with Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which the Customer acquired Customer Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under applicable Data Protection Laws.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Customer Data, the parties hereby acknowledge and agree that the Customer is the Controller and Airbrake is the Processor, and accordingly Airbrake agrees that it shall process all Customer Data in accordance with its obligations pursuant to this DPA.

2.4 Each party shall appoint an individual within its organization authorized to respond from time to time to enquiries regarding the Customer Data and each party shall deal with such enquiries promptly.

2.5 Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including applicable Data Protection Laws, in respect of its processing of Customer Data and any processing instructions it issues to Processor; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under applicable Data Protection Laws for Airbrake to process Customer Data for the purposes described in the Main Agreement**.**

2.6 Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the applicable Data Protection Law, and all communications from Regulators that relate to the Customer Data.

3. Airbrake obligations

3.1 With respect to all Customer Data, Airbrake warrants that it shall:

(a) only process Customer Data in order to provide the Service, and shall act only in accordance with Customer's documented lawful instructions as set forth in: (i) this DPA, (ii) the Customer's written instructions as represented by the Main Agreement and this DPA, and (iii) as required by applicable Data Protection Laws;

(b) as soon as reasonably practicable upon becoming aware, inform the Customer if, in Airbrake's opinion, any instructions provided by the Customer under clause 3.1(a) violate any Data Protection Laws;

(c) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Customer Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. Such measures include, without limitation, the security measures set out in Appendix 3;

(d) take reasonable steps to ensure that only authorized personnel have access to such Customer Data and that any persons whom it authorizes to have access to the Customer Data are under obligations of confidentiality;

(e) as soon as reasonably practicable upon becoming aware, notify the Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise processed by Airbrake, its Sub-Processors, or any other identified or unidentified third party (a "**Security Breach**");

(f) promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in Airbrake's possession concerning such Security Breach insofar as it affects the Customer, including the following to the extent then known:

(i) the possible cause and consequences for the Data Subjects of the Security Breach;
(ii) the categories of Customer Data involved;
(iii) a summary of the possible consequences for the relevant data subjects;
(iv) a summary of the unauthorized recipients of the Customer Data; and
(v) the measures taken by Airbrake to mitigate any damage;

(g) not make any public announcement about a Security Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable Data Protection Laws;

(h) promptly notify the Customer if it receives a request from a data subject to access, rectify or erase that individual's Customer Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Customer Data (each a "**Data Subject Request**"). Airbrake shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees. To the extent that the Customer does not have the ability to address a Data Subject Request, then upon Customer's request Airbrake shall provide reasonable assistance to the Customer to facilitate such Data Subject Request to the extent able and in line with applicable law. Customer shall cover all costs incurred by Airbrake in connection with its provision of such assistance;

(i) other than to the extent required to comply with applicable law, as soon as reasonably practicable following termination or expiry of the Main Agreement or completion of the Service, Airbrake will delete all Customer Data (including copies thereof) processed pursuant to this DPA;

(j) taking into account the nature of processing and the information available to Airbrake, provide such assistance to the Customer as the Customer reasonably requests in relation to Airbrake's obligations under applicable Data Protection Laws with respect to:

(ii) notifications to the supervisory authority under Data Protection Laws and/or communications to data subjects by the Customer in response to any Security Breach; and

(iii) the Customer's compliance with its obligations under the Data Protection Laws with respect to the security of processing; provided that the Customer shall cover all costs incurred by Airbrake in connection with its provision of such assistance.

3.2 To the extent legally required under applicable Data Protection Law, Airbrake agrees (a) to only use Customer Data to provide the Services under this DPA and the Main Agreement; (b) to not collect, retain, use, sell, share, disclose or otherwise process any Customer Data, for any purpose other than providing the Services under this DPA and the Main Agreement, or as otherwise permitted; and (c) not to combine Customer Data with Personal Data that Airbrake receives from or on behalf of another person or entity or collects from its own interactions with a Data Subject except to perform the Services. Notwithstanding anything to the contrary in this DPA and the Main Agreement, Customer acknowledges that Airbrake shall have a right to Process Customer Data in relation to the support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent Airbrake deidentifies Customer Data, it will take reasonable measures to ensure that the information cannot be associated with an individual, publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify it, and contractually obligate any recipients of the deidentified information to comply with all provisions in this paragraph. Airbrake shall promptly inform Customer if it determines that it can no longer meets its obligations in this section. Airbrake hereby certifies that it understands its obligations in this section and will comply with them. For the purposes of this section, "sell" and "share" shall have the meanings ascribed to them in the California Privacy Law.

4. Sub-processing

4.1 The Customer grants a general authorization to Airbrake to appoint third party data center operators, and outsourced marketing, business, engineering and customer support providers as Sub-Processors to support the performance of the Service.

4.2 Airbrake will provide, upon written request, a list of Sub-Processors to the Customer.

4.3 Airbrake will ensure that any Sub-Processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub- processor terms substantially no less protective of Customer Data than those imposed on Airbrake in this DPA (the "**Relevant Terms**"). Airbrake shall procure the performance by such Sub-Processor of the Relevant Terms and shall be liable to the Customer for any breach by such person of any of the Relevant Terms.

4.4 To the extent Customer reasonably believes the new Sub-Processor's Processing of Customer Data may violate applicable Data Protection Laws or weaken the security of Customer Data, Customer may object in writing to Processor's new Sub-Processor by notifying Airbrake within ten (10) days after notification described in Section 5(b). Any such written objection shall include Customer's specific reasons for its objection and proposed options to mitigate alleged risk, if any. In such event, Airbrake will either (i) instruct the Sub-Processor to cease any further processing of Customer Data, in which event this DPA shall continue unaffected, or (ii) allow Customer to terminate this DPA. In the event of termination by Customer pursuant to this Section, Customer shall not be entitled to a pro-rata refund of the remuneration for the Services, unless the objection is based on justified reasons of non-compliance with applicable Data Protection Law. In the absence of timely and valid objection by Customer, such Sub-Processor may be commissioned to process Customer Data.

5. Audit and records

5.1 Airbrake shall, in accordance with Data Protection Laws, make available to the Customer such information in Airbrake's possession or control as the Customer may reasonably request with a view to demonstrating Airbrake's compliance with the obligations of data processors under applicable Data Protection Laws in relation to its processing of Customer Data. Subject to obligations of confidentiality, Airbrake will make available to Customer a summary of its most recent relevant audit report and/or other documentation reasonably required by Customer which Airbrake makes generally available to its customers, so that Customer can verify Processor's compliance with this DPA.

5.2 To the extent that the Customer considers that such reports do not sufficiently verify Airbrake's compliance with its obligations under this DPA, Customer may audit Airbrake's compliance with this DPA up to once per year, unless otherwise requested by a Supervisory Authority. Such an audit will be conducted by an independent third party ("Auditor") reasonably acceptable to Airbrake. Before the commencement of any such on-site audit, Customer must submit in writing a detailed proposed audit plan to Airbrake at least 30 business days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration and date of the audit, as well as the proposed Auditor. Airbrake will review the proposed audit plan and provide Customer with any concerns or questions and will work cooperatively with Customer to agree on a final audit plan before the proposed audit date. Prior to the start of an audit, the parties will agree to reasonable time, duration, place and manner conditions for the audit. The results of the inspection and all information reviewed during such inspection will be deemed Airbrake's confidential information. Notwithstanding any other terms, the Auditor may only disclose to the Customer specific violations of the DPA, if any, and the basis for such findings, and shall not disclose to Customer any of the records or information reviewed during the inspection.

6. Data transfers

6.1 Restricted Transfers. To the extent any processing of Customer Data by Airbrake or Customer's use of the Services involves a Restricted Transfer of Customer Data, the terms set forth in this Section apply. Insofar as the Main Agreement involves the transfer of Customer Data from any jurisdiction where applicable Data Protection Laws require that additional steps, or safeguards, be imposed before the Customer Data can be transferred to a second jurisdiction, Airbrake agrees to cooperate with Customer to take appropriate steps to comply with applicable Data Protection Laws.

6.2 EEA Personal Data. The parties agree that the Standard Contractual Clauses will apply to any Restricted Transfer of Customer Data from the EEA, either directly or via onward transfer. To the extent there is any conflict between the DPA and the applicable EU SCC in relation to the processing of EEA Personal Data, the terms of the EU SCC will prevail. To the extent applicable, the Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

a) Module Two (Controller to Processor) of the EU SCC, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, will apply where Customer is a Controller of Customer Data and Airbrake is a Processor of Customer Data. Airbrake will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter'.

b) The Customer acknowledges and accepts that the provision of the Service under the Main Agreement may require the processing of Customer Data by Sub-Processors in countries outside the EEA.

c) If, in the performance of this DPA, Airbrake transfers any Customer Data to a Sub-Processor located outside of the EEA (without prejudice to clause 4) or Switzerland, Airbrake shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as: (i) the requirement for Airbrake to execute or procure that the Sub-Processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under Data Protection Laws and set out in Appendix 2; or (ii) the existence of any other specifically approved safeguard for data transfers (as recognized under Data Protection Laws) and/or a European Commission finding of adequacy.

d) The parties agree that the following terms shall apply to Module Two of the EU SCC:

(i) in Clause 7, the optional docking clause will not apply;
(ii) certification of deletion of Customer Data that is described in Clause 8.5 of the EU SCC shall be provided by Airbrake to Customer upon request;
(iii) in Clause 9, Option 2 will apply and the time period for prior notice of Sub-Processor changes will be as set forth in the DPA;
(iv) in Clause 11, the optional language will not apply;
(v) in relation to Clause 13(a), see (x) below;
(vi) in Clause 17, Option 1 will apply, and the parties agree that EU SCC will be governed by Ireland law;
(vii) in Clause 18(b), the parties agree that disputes will be resolved before the courts of Ireland;
(viii) Annex I, Part A of the EU SCC shall be deemed completed with the information set out in Appendix 2 (List of Parties & Details of Transfer), Section A of this DPA;
(ix) Annex I, Part B of the EU SCC shall be deemed completed with the information set out in Appendix 2 (List of Parties & Details of Transfer), Section B of this DPA;
(x) in Annex I, Part C of the EU SCC, Ireland Supervisory Authority will be the competent supervisory authority;
(xi) subject to Section 3.1 of the DPA, Appendix 3 (Technical and Organizational Security Measures) of the DPA serves as Annex II of EU SCC;
(xii) subject to Section 4 of this DPA, Annex III of the EU SCC shall be deemed completed with the information set out in Appendix 2 (List of Parties & Details of Transfer), Section C of this DPA; and
(xiii) The Customer may exercise its right of audit under clause 8.9 of the standard contractual clauses as set out in, and subject to the requirements of, Section 5 of this DPA.

6.3 Swiss Personal Data**.** In accordance with guidance issued by the Swiss Federal Data Protection and Information Commissioner (FDPIC), the parties hereby agree to adopt the EU SCC as adapted herein in order to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with Article 6 paragraph 2 letter a of the Federal Act on Data Protection ("FADP"). To the extent there is any conflict between the DPA and this Section 6.3, the terms of this section will prevail in relation to Swiss Personal Data. The parties agree that in relation to Restricted Transfer of Swiss Personal Data, Section 8.3 applies except:

a) for purposes of Annex I.C under Clause 13 of the EU SCC insofar as the data transfer is governed by the FADP, the Supervisory Authority shall be Switzerland's Federal Data Protection and Information Commissioner (FDPIC); and

b) the term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in Switzerland in accordance with Clause 18(c) of the EU SCC. The EU SCC shall also protect the data of Switzerland legal entities until the entry into force of the 25 September 2020 revised version of the Federal Act on Data Protection (revised FADP). Any references in the Standard

Contractual Clauses to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA.

6.4 UK Personal Data. In respect of any UK Restricted Transfer, Customer acting on its own behalf and as agent for each Customer Affiliate (each as "data exporter") and Airbrake acting on its own behalf ("data importer") with effect from the commencement of the relevant transfer agree that such transfer(s) will be carried out in accordance with and subject to the International Data Transfer Agreement A1.0 issued by the ICO ("UK IDTA"), which can be found at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf. To the extent there is any conflict between the DPA and the UK IDTA in relation to the processing of UK Personal Data, the terms of the UK IDTA will prevail. To the extent applicable, the UK IDTA will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

Part 1: Tables

Table 1: Parties and Signatures. See Appendix 2.

Table 2: Transfer Details

UK country's law that governs the IDTA	☒ England and Wales
Primary place for legal claims to be made	☒ England and Wales
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller
The status of the Importer	In relation to the Processing of the Transferred Data: ☒ Importer is the Exporter's Processor or Sub-Processor
Whether UK GDPR applies to the Importer	☒ UK GDPR applies to the Importer's Processing of the Transferred Data
Linked Agreement	Name of agreement: Main Agreement Date of agreement: See Term Effective Date. Parties to the agreement: See Appendix 2 Reference (if any): N/A
Term	The Importer may Process the Transferred Data for the following time period: ☒ the period which the Importer retains the Transferred Data
Ending the IDTA before the end of the Term	☒ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing, or any termination provisions contained in the Agreement or DPA apply.
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2 of the IDTA: ☒ Exporter
Can the Importer make further transfers of the Transferred Data?	☒ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 of the IDTA (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1 of the IDTA: ☒ to the authorised receivers (or the categories of authorised receivers) and other third parties as described in the DPA.
Review Dates	First review date: Terms Effective Date of the DPA The Parties must review the Security Requirements at least once:

	☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment, to the extent that Importer is made aware of such changes; Importer will conduct a review at the time of contract renewal.

Table 3: Transferred Data. See Appendix 2, which will be updated automatically if the data transferred changes.

Table 4: Security Requirements. See Appendix 3, which will update automatically if the information is updated in the Agreement or this DPA.

1.1.1. Part 2: Extra Protection Clauses: N/A.

1.1.2. Part 3: Commercial Clauses: See the parties' Main Agreement to which this DPA is attached and incorporated by reference.

1.1.3. Part 4: Mandatory Clauses: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

7. General

7.1 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Customer Data.

7.2 Airbrake's liability under or in connection with this DPA (including under the standard contractual clauses set out in Appendix 2) is subject to the limitations on liability contained in the Main Agreement.

7.3 This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

7.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts of San Francisco, California.

7.5 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Customer: _____

Signature _____

Name _____

Title _____

Date Signed _____

Airbrake Technologies Holdings, Inc.

Signature _____

Name _____

Title _____

Date Signed _____

Appendix 1
Details of the Customer Data and Processing Activities

a) The Customer Data comprises: in relation to visitors of the Customer's online properties identification data, connection data, or localization data (including IP addresses). Customer, its online visitors and/or other partners may also upload content to Customer's online properties which may include personal data and special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion.
b) The duration of the processing will be: until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable);
c) The processing will comprise: Processing necessary to provide the Service to Customer, pursuant to the Main Agreement ;
d) The purpose(s) of the processing is/ are: necessary for the provision of the Service;
e) Customer Data may concern the following data subjects:
    - Prospective customers, customers, resellers, referrers, business partners, and vendors of the Customer (who are natural persons);
    - Employees or contact persons of the Customer's prospective customers, customers, resellers, referrers, Sub-Processors, business partners, and vendors (who are natural persons);
    - Employees, agents, advisors, and freelancers of the Customer (who are natural persons); and/or Natural persons authorized by the Customer to use the Service.

Appendix 2
List of Parties & Details of Transfer

A. LIST OF PARTIES

Data exporter(s):

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Processing Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and Airbrake

Role: Controller

Data importer(s):

Name: **Airbrake Technologies Holdings, Inc.**

Address: 98 San Jacinto Blvd, Suite 1300, Austin, TX 78701

Contact person's name, position and contact details: Richard Huddleston, Director of Engineering, richard.huddleston@logicmonitor.com

Activities relevant to the data transferred under these Clauses: Processing Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and Airbrake

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects (please specify):
The data exporter may submit Personal Data to Airbrake, 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 categories of data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);
- Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);
- Employees, agents, advisors, and freelancers of the data exporter (who are natural persons); and/or
- Natural persons authorized by the data exporter to use the services provided by Airbrake to the data exporter.

Categories of personal data transferred

The data exporter may submit Personal Data to Airbrake, 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:

Names, contact information (email, phone, fax, physical address etc.), identification data, or localization data (including

IP addresses).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data exporter may submit special categories of data to Airbrake, the extent of which is determined and controlled by the data exporter in its sole discretion.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

The nature of the processing of Personal Data by Airbrake is performance of the Services set forth in the Main Agreement.

Purpose(s) of the data transfer and further processing

The objective of the processing of Personal Data by Airbrake is to provide the Service, pursuant to the Main Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration of the processing will be: until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable)

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
See Appendix 2, Section C of this DPA.

C. SUB-PROCESSORS

Sub-processor Name	**Description of Processing** (including a clear delimitation of responsibilities in case several subprocessors are authorised)	**Location of Processing**
HubSpot	Used for customer relationship management (CRM). HubSpot processes customer account information, including name and email for any users that have accounts in Airbrake. Continuous basis.	Massachusetts, United States
Slack	When new Airbrake users sign up for an account, there is a Slack notification with the name of the account and a link back to HubSpot.	San Francisco, United States Dublin, Ireland
Amazon Web Services	AWS is used to store customer data, which may include personal data shared with AWS. Continuous basis.	Determined by Customer / Data Controller's Selected Location

Appendix 3

Technical and Organizational Security Measures

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Security Measures

1. Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.
2. More specifically, data importer/sub-processor's security program shall include:

Infrastructure Security

1. The company's infrastructure resides on Amazon Web Services and is segregated per environment into separate VPCs, separate regions and at least two availability zones.
2. AWS Access . Access to Amazon Web Services uses IAM policies to implement limited Role Based Access Control and 2FA.
3. Application and services are segregated by tiered network access control lists (public, protected, and private networks). Network traffic is further restricted by security groups applicable to the type of host and services or applications it may need to interact with.
4. Network Access Control Lists

Access Control of Data Processing Systems

Data importer/sub-processor untilizes Amazon Web Services ("**AWS**") for company infrastructure. AWS has robust data privacy and security procedures to protect customer data as outlined here: https://aws.amazon.com/compliance/eu-data-protection/. No employees of the Data importer have any direct physical access to the servers or equipment that processes or stores data from the exporter.

Access Control to Data Processing Systems

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- all access to data content is logged, monitored, and tracked
- role-based access controls with 2 factor authentication, including:

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization). This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and
- control of files, controlled and documented destruction of data.

Availability Control

Data importer/Sub-Processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- use of multiple availability zones in AWS

Transmission Control

Data importer/Sub-Processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- data encrypted in transmission and at rest
- as far as possible, data transmissions are logged, monitored and tracked.

Documentation

Data importer/Sub-Processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/Sub-Processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Appendix 4

Transfer Impact Assessment: United States

As the Data Importers are located in the United States, which does not have an adequacy determination from the European Union, the following information is documented in support of the Parties' warranty pursuant to Clause 14(a): "(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses."

Clause 14 requires the Parties to consider "the specific circumstances of the transfer," as well as "the laws and practices of the third country" and the "relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses".

Taking account of these instructions and the guidance furnished by the European Data Protection Board (Recommendations 1/2020, 18 June 2021) following the Judgment of the Court of Justice of the European Union (CJEU) in the "*Schrems II"* proceeding, the Parties observe or represent as follows:

United States Law and Practice

In the US, as in other jurisdictions, there is always the possibility that Data Importer could receive a judicial subpoena or warrant seeking information in connection with a civil or criminal proceeding, or a demand for information relating to an investigation by a regulatory body. These will be reported to Customer in the EEA (unless prohibited by law) and are subject to objections and recourse under principles of "fair process" in the US, much as they would be in Europe.
The CJEU *Schrems II* Judgment did not express concern that such procedures are outside the norms in democratic societies or result in an inability to comply with a commitment to safeguard the privacy of personal information. Rather, the Judgment focuses on these particular US federal measures:

- Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702"), a statute establishing procedures to authorize national security surveillance programs to collect foreign intelligence from non-US persons located outside the US (and thus not covered by constitutional Fourth Amendment search-and-seizure rights). The FISA Court (staffed by independent, life-tenured federal judges) reviews and approves the procedures designed to target foreign suspects and minimize data collection and dissemination. Law enforcement or security agencies, chiefly the Federal Bureau of Investigation, may serve private companies with directives, typically in the form of "national security letters," under an authorized surveillance program without requiring a warrant. These order the disclosure of specified communications data such as emails or telephone call logs.

- Executive Order 12333 ("EO 12333"), a general directive organizing US intelligence activities, including electronic surveillance that the National Security Agency (NSA) conducts outside the US. Presidential Policy Directive 28 (PPD-28, 2014) limits "signals intelligence" operations to a "foreign intelligence or counterintelligence purpose."

US law and practice under these measures is detailed in the September 2020 inter-agency White Paper prepared jointly by the US Departments of Justice and Commerce and the Office of the Director of National Intelligence, https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF hereinafter "**White Paper**"). It points out that most companies do not deal in data that is of any interest to US intelligence agencies, and that information gathered from companies under FISA 702 orders "to counter threats such as terrorism, weapons proliferation, and hostile foreign cyber activity" is frequently shared with EU Member States and serves EU public interests. The inter-agency White Paper references public information available about privacy protections in the US concerning government access to data.

FISA 702

Under FISA 702, the US Attorney General and the Office of the Director of National Intelligence ("ODNI") may submit a written certification to the FISA Court for approval for up to one year, authorizing a program for the targeted collection

of communications data of non-US persons outside the US for specified foreign intelligence purposes, such as surveillance for terrorism or the acquisition of weapons of mass destruction. The program must specify how a "selector" (an account identifier such as an individual's email address or telephone number) may be "tasked" to acquire the type of foreign intelligence specified in the certification. If the certification is approved by the FISA Court, the FBI or other agencies may issue directives to relevant companies, most often telecommunications or electronic communications services providers, demanding the disclosure of communications data based on the tasked selectors.

The requesting government agency must record the reasons why each person was targeted. Each targeting assessment made by NSA analysts, for example, and each selector tasked for data acquisition is reviewed by independent intelligence oversight attorneys in the Department of Justice for compliance with the applicable legal standard defined in the targeting procedures approved by the FISA Court. The Department of Justice attorneys performing this function are responsible for reporting compliance incidents to the FISA Court. The Department of Justice and ODNI conduct bimonthly reviews and report to the FISA Court semiannually on compliance incidents and remedial measures, such as data purging, regardless of the nationality of the affected individual. Summaries are made public and affect the annual reauthorization process before the FISA Court. The US Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent federal oversight entity established under the 9/11 Commission Act of 2007, has also conducted longer- term reviews of this process, as well as semi-annual reports. These are published at www.pclob.gov. The independence of FISA Court review is reflected in two FISA Court opinions in 2019 and 2020 taking exception to certain government practices. See https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf and https://www.intelligence.gov/index.php/ic-on-the-record-database/results/1008-release-of-documents-related-to-the-temporary-retention,-use,-and-disclosure-of-unlawful-fisa- The first of these involves what the Court considered to be overbroad use of an approved program, while the second concerns the retention of data improperly obtained about a specific individual. Both illustrate that the FISA Court does indeed have an active and effective role in supervising warrantless surveillance activities, in addition to the roles of the Department of Justice, the Inspectors General, and the PCLOB.

In 2018 the US Congress adopted legislation, signed by the President, that introduced new privacy safeguards to the FISA 702 regime by amending FISA and other statutes. These require (1) data querying procedures to access collected data (in addition to targeting and minimization procedures), which must be approved with annual program certification, (2) congressional notification and other steps before agencies seek to collect communications "about" a targeted selector (i.e., referring to a selector in the content rather than simply including the selector in the address as at present), (3) expanding the oversight functions of the PCLOB, (4) requiring the FBI and NSA to maintain their own Privacy and Civil Liberties Officers, with procedures to handle related complaints from individuals, (5) extending whistleblower protections to contract workers at intelligence agencies, and (6) expanding disclosure and reporting requirements. These changes are not reflected in the *Schrems II* Judgment, but they substantially improve privacy protection for all affected individuals, including EEA residents.

The CJEU questioned whether US law provides for legal redress for non-US persons in the event of violations of FISA 702. In fact, the FISA statute provides for compensatory and punitive damages, and for the recovery of attorney's fees, if intercepted communications are used or disclosed unlawfully (50 U.S.C. § 1810). Compensatory damages and attorney's fees could also be available in a civil action under the Electronic Communications Privacy Act (18 U.S.C. § 2712). More generally, a person suffering "legal wrong" because of the conduct of a government official can bring an action for damages under the Administrative Procedure Act (APA) (5 U.S.C. § 702). (In 2020 Wikimedia Foundation has an APA claim against NSA challenging data collection under a FISA 702 directive, which is pending appeal before the US 4th Circuit Court of Appeals, No. 20-1191).

EO 12333 and PPD-28

The White Paper observes that EO 12333 does not authorize the US security agencies to require US private companies to disclose personal information. They may choose to cooperate voluntarily in an investigation, but they are not obliged to do so absent a warrant or a FISA 702 order. The CJEU expressed concern in the *Schrems II* Judgment that EO 12333 could result in the "bulk collection" of PERSONAL INFORMATION, but companies cannot be compelled to participate in such bulk collection: EO 12333 does not oblige them to, and warrantless demands under FISA 702 programs require targeted and minimized data collection.

The White Paper points out that private companies cannot be expected to know whether the intelligence services of the US (or other countries) are *covertly* surveilling their communications abroad, but (a) companies may use security techniques to detect interception of their communications and protect the content of their communications and databases and (b) PPD-28 imposes relevant limits on US covert foreign communications surveillance. It must be

limited to detecting and countering "(1) espionage and other threats from foreign powers; (2) terrorism; (3) threats from weapons of mass destruction; (4) cybersecurity threats; (5) threats to US or allied forces; and (6) transnational criminal threats." Further, each US intelligence agency is required under PPD-28 to adopt procedures allowing the retention or dissemination of personal information (regardless of the nationality of the person) only to the extent the retention or dissemination of "comparable information concerning U.S. persons would be permitted." As described in the White Paper, each intelligence agency is required to document its PPD-28 procedures, typically including senior executive approvals and documented privacy protections for any bulk data collection. The relevant Central Intelligence Agency Guidelines were issued in 2017 and are publicly available (but they were not available at the time of the 2016 EU Privacy Shield decision and are not addressed in the *Schrems II* Judgment). Some intelligence agency Inspector General reports are also available, indicating reports on compliance audits and remedial actions over a period of years at the NSA and CIA.

It is difficult for a private company to make an "equivalency" comparison with the EEA, because there is little publicly available information in the various EU / EEA Member States to compare actual practices in authorizing and conducting international communications surveillance. However, only about half of the EU Member States required any form of judicial review for the collection of personal data by intelligence services, according to a report by FRA, the European Union Agency for Fundamental Rights, https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-volume-i-member-states-legal-frameworks. The White Paper documents instances where the European Court of Human Rights has upheld national *domestic* intelligence surveillance programs in EU Member States including bulk interception of communications based on keyword searches, with executive rather than judicial review, and not addressing unfettered foreign surveillance.

By comparison, the US laws described above involve more oversight, individual targeting, data minimization, and potential correction and redress. It is fair to conclude that the level of privacy protection with respect to data access by government authorities in the US is at least equivalent to the prevailing standards in the EEA.

Experience of Customer and Data Importer

As noted in the US interagency White Paper, private companies engaged in commerce are not typically subjects of interest to US intelligence agencies concerned with counter-terrorism, weapons proliferation, and "hostile foreign cyber activity." According to the White Paper, such requests are rare, and they have been focused on terrorist threats.
Consistent with that assessment, Customer and Airbrake have not received FISA national security letters seeking personal information in its custody or control about EEA residents.

Supplementary Measures to Assure Safeguards of Privacy

The Data Importer's technical and organizational security measures are summarized in Annex II. Data will be encrypted when transferred between Customer and the Data Importer. Both Customer and Data Importer employ anti-threat services that scan for malware and unauthorized access, as well as running regular penetration tests and monitoring for vulnerabilities. Thus, even official surveillance is likely to be detected. If this were to occur, Data Importer is obliged to report the suspected intrusion to Customer.

Although the risk is low that the personal information transferred to Data Importer in the US would be targeted for surveillance by US (or other) intelligence authorities, there are supplementary measures that Data Importer undertakes to meet its obligations to protect the confidentiality of European personal information:

- Data Importer warrants that it has not designed its systems and applications with "backdoors" to provide access on demand to government authorities, nor will it furnish source code or encryption keys to any government agency so that it can access client data except as required by law and through legal process.

- Data Importer will promptly notify Customer if it receives a demand for disclosure of personal information, so that Customer may attempt to limit or prevent disclosure, unless Data Importer is prohibited from notifying others under applicable law.

- Data Importer will take appropriate legal action to challenge demands for disclosure of personal information, including efforts to limit or prevent disclosure where possible or obtain relief under mutual assistance treaties where compliance could put Data Importer or Customer in breach of foreign data protection law.

- Data Importer will maintain security procedures, as outlined in Annex II, that protect data in transit and at rest and detect and protect against interception and penetration. Where practicable, Data Importer will secure personal information data elements with anonymization techniques such as data hashing or by pseudonymization or data masking. Where encryption is used, Data Importer will use appropriate key management protocols to maintain the effectiveness of the protection. Data Importer will require appropriate verification of identification credentials of law enforcement officials and secure means of communicating with them or transferring any data as required to them.

- These policies and procedures are managed at Data Importer by its legal team in coordination with its data privacy and security teams.