HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Exhibits A and B, and Appendices 1 and 2.

2. This DPA has been pre-signed on behalf of SignalFx. The Standard Contractual Clauses in Exhibit B have been pre-signed by SignalFx as the data importer. This DPA will be null and void if any changes are made to it beyond filling out the sections described in 3, below.

3. To complete this DPA, Customer must:

    a. Complete the information in the signature box and sign on Page 8.
    b. Complete the information as the data exporter on Page 10 and Page 19.
    c. Complete the information in the signature box and sign on Page 18 and Page 20.

4. Send the completed and signed DPA to SignalFx by email to: gdpr-compliance@signalfx.com. Upon receipt of the validly completed DPA by SignalFx at this email address, this DPA will become legally binding.

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part of the Master Services Agreement/Services Agreement (the "**Agreement**") between SignalFx, Inc. ("**SignalFx**") and [Customer name] ("**Company**") (collectively the "**Parties**").

1. Subject Matter and Duration.

a) Subject Matter. This DPA reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Company Personal Data in connection with SignalFx's execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing DPA will have the meanings given to them in the Agreement. If and to the extent language in this DPA or any of its Exhibits conflicts with the Agreement, this DPA shall control.

b) Duration and Survival. This DPA will become legally binding upon the Effective Date of the Agreement or upon the date that the Parties sign this DPA if it is completed after the effective date of the Agreement. SignalFx will Process Company Personal Data until the relationship terminates as specified in the Agreement. SignalFx's obligations and Company's rights under this DPA will continue in effect so long as SignalFx Processes Company Personal Data.

2. Definitions.

For the purposes of this DPA, the following terms and those defined within the body of this DPA apply.

a) "**Applicable Data Protection Law(s)**" means the relevant data protection and data privacy laws, rules and regulations to which the Company Personal Data are subject. "Applicable Data Protections Law(s)" shall include, but not be limited to, the EU General Data Protection Regulation 2016/679 ("**GDPR**").

b) "**Company Personal Data**" means Personal Data pertaining to Company's users or employees located in the European Economic Area Processed by SignalFx. The Company Personal Data and the specific uses of the Company Personal Data are detailed in **Exhibit A** attached hereto, as required by the GDPR.[1]

c) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

d) "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

e) "**Process**" or "**Processing**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated 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.

f) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Company Personal Data on behalf of Company subject to this DPA.

g) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Personal Data Processed by SignalFx.

h) "**Services**" means any and all services that SignalFx performs under the Agreement.

i) "**Third Party(ies)**" means SignalFx's authorized contractors, agents, vendors and third party service providers (i.e., sub-processors) that Process Company Personal Data.

3. Data Use and Processing.

a) Compliance with Laws. Company Personal Data shall be Processed in compliance with the terms of this DPA[2] and all Applicable Data Protection Law(s).[3]

b) Documented Instructions. SignalFx and its Third Parties shall Process Company Personal Data only in accordance with the documented instructions of Company or as specifically authorized by this DPA, the Agreement, or any applicable

---

[1] GDPR Requirement: Art. 28(3) (Agreement must set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects.)

[2] GDPR requirement: Art. 28(3) ("Processing by processor shall be governed by a contract."); Privacy Shield Supplemental Principle 10(a)(i) (Contract required for any Processing in the United States.)

[3] GDPR requirement: General compliance with GDPR; and Art. 28(1) (Processor guarantees.)

Statement of Work.[4] SignalFx will, unless legally prohibited from doing so, inform Company in writing if it reasonably believes that there is a conflict between Company's instructions and applicable law or otherwise seeks to Process Company Personal Data in a manner that is inconsistent with Company's instructions.

c) Authorization to Use Third Parties. To the extent necessary to fulfill SignalFx's contractual obligations under the Agreement or any Statement of Work, Company hereby authorizes (i) SignalFx to engage Third Parties and (ii) Third Parties to engage sub-processors.[5] Any Third Party Processing of Company Personal Data shall be consistent with Company's documented instructions and comply with all Applicable Data Protection Law(s).[6]

d) SignalFx and Third Party Compliance. SignalFx agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties' Processing of Company Personal Data that imposes on such Third Parties (and their sub-processors) data protection and security requirements for Company Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Company for SignalFx's Third Parties' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Company Personal Data.[7] SignalFx shall flow down all obligations in this DPA to Third Parties (and their sub-processors) regarding, among other things: (i) Company Personal Data and (ii) all Company's and Company's regulator's rights regarding review and audit (including Company's right to appoint an independent third party to perform such review or audits).

e) Right to Object to Third Parties. SignalFx shall make available to Company a list of Third Parties that Process Company Personal Data upon reasonable request. Prior to engaging any new Third Parties that Process Company Personal Data, SignalFx will notify Company via email[8] and allow Company thirty (30) days to object.[9] If Company has legitimate objections to the appointment of any new Third Party, the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Company may terminate the part of the service performed under the Agreement that cannot be performed by SignalFx without use of the objectionable Third Party.

---

[4] GDPR requirement: Art. 28(3)(a) (Processor can only process Personal Data on Controller's documented instructions and Privacy Shield Supplemental Principle 10(a)(ii)(1) (Processor can act only on instructions from Controller.)

[5] GDPR requirement: Art. 28(2) (Processor can engage another processor with general written authorization of the controller.)

[6] GDPR requirement: Art. 28(4) (Subprocessor must have same contractual obligations imposed on it as processor.)

[7] GDPR requirement: Art. 28(4) (see last sentence) (Processor is responsible for subprocessors' actions.)

[8] GDPR Art 28(2) does not specify what constitutes proper notice. Posting updates on a URL referenced in the DPA may be sufficient.

[9] GDPR requirement: Art. 28(2) (Processor must give notice of any new or replacement sub-processors and allow Controller to object.)

f) Confidentiality. Any person or Third Party authorized to Process Company Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.[10]

g) Personal Data Inquiries and Requests. SignalFx agrees to comply with all reasonable instructions from Company related to any requests from individuals exercising their rights in Personal Data granted to them under Applicable Data Protection Law(s)[11] ("**Privacy Request**"). At Company's request and without undue delay, SignalFx agrees to assist Company in answering or complying with any Privacy Request in so far as it is possible.[12]

h) Data Protection Impact Assessment and Prior Consultation. SignalFx agrees to provide reasonable assistance at Company's expense to Company where, in Company's judgement, the type of Processing performed by SignalFx is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.[13]

i) Demonstrable Compliance. SignalFx agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s)[14] and provide any necessary records to Company to demonstrate compliance upon reasonable request.[15]

4. Cross-Border Transfers of Personal Data.

a) Cross-Border Transfers of Personal Data. Company authorizes SignalFx and its Third Parties to transfer Company Personal Data across international borders, including from the European Economic Area to the United States.[16] Any cross-border transfer of Company Personal Data must be supported by an approved adequacy mechanism.

b) Standard Contractual Clauses. SignalFx and Company will use the Standard Contractual Clauses in **Exhibit B** as the adequacy mechanism supporting the transfer and Processing of Company Personal Data.

5. Information Security Program.

a) SignalFx agrees to implement appropriate technical and organizational measures

---

[10] GDPR requirement: Art. 28(3)(b) (Processor and Subprocessor are subject to duty of confidence.)

[11] GDPR requirement: Art. 28(3)(e)(Processors must assist Controllers with complying with Controllers' obligations to respond to data subjects' requests to exercise their data subject rights under the GDPR) and Privacy Shield Supplemental Principle 10(a)(ii)(3) (Assist Controller in responding to individuals exercising their rights under the Privacy Shield.)

[12] GDPR requirement: Art. 28(3)(e)(Processors must assist Controllers in complying with Controllers' obligations to respond to data subjects' requests to exercise their data subject rights under the GDPR) and Privacy Shield Supplemental Principle 10(a)(ii)(3) (Assist Controller in responding to individuals exercising their rights under the Privacy Shield.)

[13] GDPR requirement: Art. 28(3)(f) (Processor must assist Controller with complying with Articles 32-36), 35 (DPIAs), 36 (Prior Consultation).

[14] GDPR requirement: Art. 30(2) (Processors must retain records of processing activities.)

[15] GDPR requirement: Art. 28(3)(h) (Processor must make available to the controller all information necessary to demonstrate compliance with Art. 28.)

[16] GDPR Requirement: Art. 28(3)(a): (Processor instructions must include reference to transfers of personal data to a third country.)

designed to protect Company Personal Data as required by Applicable Data Protection Law(s) (the "**Information Security Program**").[17] Such measures shall include:

i) Encryption of Company sensitive data in transit and at rest;

ii) The ability to ensure the ongoing confidentiality, integrity, availability of SignalFx's Processing and Company Personal Data;

iii) The ability to restore the availability and access to Company Personal Data in the event of a physical or technical incident;

iv) A process for regularly evaluating and testing the effectiveness of the Company's Information Security Program to ensure the security of Company Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.[18]

6. Security Incidents.

a) Security Incident Procedure. SignalFx will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes,[19] and (ii) restore the availability or access to Company Personal Data in a timely manner.[20]

b) Notice. SignalFx agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) (but in no event longer than seventy-two (72) hours) to Company's Designated POC if it knows or reasonably suspects that a Security Incident has taken place.[21] Such notice will include all available details required under Applicable Data Protection Law(s) for Company to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.[22]

7. Audits.

a) Right to Audit; Permitted Audits. In addition to any other audit rights described in the Agreement, Company and its regulators shall have the right to an on-site audit of SignalFx's architecture, systems, policies and procedures relevant to the

---

[17] GDPR requirement: Art. 28(1) (Processors to guarantee to implement appropriate technical and organizational measures to process personal data as required under the GDPR and ensure protection of rights of the data subject; Art. 32 (Obligations to provide secure Processing) and Privacy Shield Supplemental Principle 10(a)(ii)(2) (Processor to provide appropriate technical and organizational measures).

[18] GDPR Requirement**:** Art. 32(1)(a)-(d) (Security of Processing – High level overview of Information Security Program Requirements.)

[19] Not explicitly required under the GDPR but can be reasonably inferred from GDPR Art. 32(1)(c) (Implement ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services).

[20] GDPR Requirement: Art. 32(1)(c) (Implement ability to restore availability and access to personal data in a timely manner in case of an incident).

[21] GDPR requirement: Art. 28(3)(f) (Processor obligations to assist Controller with requirements of Art. 32-36) and Art. 33(2) (Breach notification: requires Controller to notify supervisory authority within **72 hours** of incident.). For negotiations: this should never be more than 48 hours so that Company can meet the breach window.

[22] GDPR requirement: Art. 33(3) (Required content of notice to supervisory authority.)

security and integrity of Company Personal Data,[23] or as otherwise required by a governmental regulator only:

i) In the event that SignalFx has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with SOC 2v Type 2 or other standards.

ii) A Personal Data Breach has occurred;

iii) An audit is formally requested by Company's data protection authority; or

iv) Mandatory Data Protection Law provides Company with a direct audit right and provided that Company shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

b) Scope of Audit. Company shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Company audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Company shall provide the results of any audit to SignalFx.

c) Cost of Audits. Company shall bear the costs of any audit. If an audit determines that SignalFx has materially breached its obligations under the DPA, SignalFx will promptly remedy the breach at its own cost.

d) Third Parties. In the event that Company conducts an audit through a third party independent auditor or a third party accompanies Company or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect SignalFx's and SignalFx's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

e) Audit Results. Upon SignalFx's request, after conducting an audit, Company shall notify SignalFx of the manner in which SignalFx does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein. Upon such notice, SignalFx shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Company when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Company may conduct a follow-up audit within six (6) months of SignalFx's notice of completion of any necessary changes. To the extent that a SignalFx audit and/or Company audit identifies any material security vulnerabilities, SignalFx shall remediate those vulnerabilities within fifteen (15) days of the completion of the

[23] GDPR requirement: Art. 28(3)(h) (Processor must allow for audits by the Controller or its representative.)

applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

8. Data Storage and Deletion.

a) Data Storage. SignalFx will abide by the following with respect to storage of Company Personal Data:

i) SignalFx will not store or retain any Company Personal Data except as necessary to perform the Services under the Agreement.

ii) SignalFx will (i) inform Company in writing of all countries where Company Personal Data is Processed or stores and (ii) obtain consent from Company for Processing or storage in the identified countries. As of the Effective Date, SignalFx stores Company Personal Data in the following countries to which Company hereby consents: United States.

b) Data Deletion.[24] SignalFx will abide by the following with respect to deletion of Company Personal Data:

i) Within thirty (30) calendar days of the Agreement's expiration or termination, or sooner if requested by Company, SignalFx will securely destroy (per subsection (iii) below) all copies of Company Personal Data (including automatically created archival copies). [25]

ii) Upon Company's request, SignalFx will promptly return to Company a copy of all Company Personal Data within thirty (30) days and, if Company also requests deletion of the Company Personal Data, will carry that out as set forth above.

iii) All deletion of Company Personal Data must be conducted in accordance with best practices for deletion of sensitive data. For example, secure deletion from a hard drive is defined at a minimum as a seven-pass write over the entire drive.

iv) Upon Company's request, SignalFx will provide a "Certificate of Deletion" certifying that SignalFx has deleted all Company Personal Data. SignalFx will provide the "Certificate of Deletion" within thirty (30) days of Company's request.

9. Contact Information.

a) SignalFx and the Company agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- SignalFx Designated POC: Marzena Fuller, CSO

[24] GDPR requirement: Art. 28(3)(g) (Processor's data deletion obligations.)

[25] GDPR requirement: Art. 28(3)(g) (Processor's obligations to delete or return of personal data.)

- Company Designated POC:_____

[COMPANY]

Signature: _____

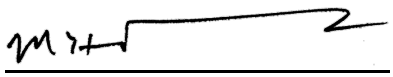
Printed Name: _____

_____

Title: _____

Date: _____

SignalFx, Inc.

Signature: 

Printed Name: Mark H. Resnick

Title: Chief Financial Officer

Date: June 8, 2018

Exhibit A

1.1 Subject Matter of Processing	The subject matter of Processing is the Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	Includes the following: ● Prospects, customers, business partners and vendors of Company (who are natural persons) ● Employees, agents, advisors, freelancers of Company, job applicants (who are natural persons) ● Company's users authorized by Company to use the Services
1.4 Nature and Purpose of Processing	The purpose of Processing of Company Personal Data by SignalFx is the performance of the Services pursuant to the Agreement.
1.5 Types of Personal Information	● Identification Data (notably email addresses and phone numbers) ● Electronic identification data (notably IP addresses and mobile device IDs)

Exhibit B

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: [INSERT Company's full legal name]

Address: [INSERT Company's address]

Tel.:_____

fax:_____

e-mail:_____

Other information needed to identify the organization:

_____

_____

_____

(the data **exporter**)

And

[*The gaps below are populated with details of the relevant Contracted Processor:*]
Name of the data importing organization: SignalFx, Inc.

Address: 60 E 3rd Ave, San Mateo, CA 94401, USA

Tel.: +1 650-539-8650; e-mail: gdpr-compliance@signalfx.com

Other information needed to identify the organization: n/a
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and 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:
[*Populated with details of, and deemed signed 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: _____

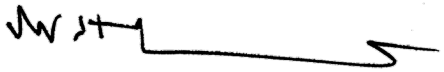
Date: _____

On behalf of the data importer:
[*Populated with details of, and deemed signed on behalf of, the data importer:*]
Name (written out in full): Mark H. Resnick

Position: Chief Financial Officer

Address: 60 E 3rd Ave, San Mateo, CA 94401, USA

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

Signature: 

Date: June 8, 2018

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:_____

Data importer
The data importer is: SignalFx, Inc.

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

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees, job applicants, agents, advisors, freelancers of data exporter (who are natural persons)

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

- First and last name
- Email address
- ID data
- Connection data
- Localization data
- Professional life data
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)

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

The objective of processing of personal data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data exporter:*]

Name: _____

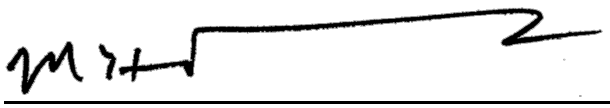
Signature: _____

Date: _____

DATA IMPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data importer:*]

Name: Mark H. Resnick, Chief Financial Officer

Signature: 

Date: June 8, 2018

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Company Personal Data, as described in the Data Processing DPA. Data Importer will not materially decrease the overall security of the Services during a subscription term.