APPNETA, INC.
DATA PROCESSING ADDENDUM FOR CUSTOMERS

This Data Processing Addendum ("**DPA**") is made and entered into between AppNeta, Inc. ("**Company**") and [] ("**Customer**") and forms part of each agreement under which Company Processes any Customer Personal Data as part of performing its obligations (the "**Services**") to Customer under that agreement (each, the "**Agreement**"). As to each such Agreement, this DPA is coterminous with the Agreement.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Company Processes Customer Personal Data for which such Authorized Affiliates qualify as the Data Controller (or Data Processor, where Company is the Subprocessor, as applicable).

Capitalized terms used in this DPA shall have the meanings set forth in this DPA. Except as modified below, the terms of the Agreement shall remain in full force and effect. In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as a DPA to the Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

- "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with the applicable party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- "**Authorized Affiliate**" means any Customer's Affiliate that is (a) subject to Data Protection Laws, and (b) permitted to use the Services pursuant to the Agreement, but has not signed its own order form and is not a "Customer" as defined in the Agreement.
- "**Contracted Processor**" means Company or a Subprocessor.
- "**Customer Group Member**" means Customer or any Authorized Affiliate.
- "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Customer Group Member pursuant to or in connection with the Agreement.
- "**Data Protection Laws**" means all laws and regulations of the European Union ("EU"), the European Economic Area ("EEA") and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement, including EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
- "**GDPR**" means EU General Data Protection Regulation 2016/679.
- "**Privacy Shield**" means the EU-US Privacy Shield Framework, as administered by the US Department of Commerce and as approved by the European Commission.
- "**Restricted Transfer**" means:
    - a transfer of Customer Personal Data from any Customer Group Member to a Contracted Processor; or

- an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer is permitted under the Agreement but would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of a legal transfer mechanism to be established under this DPA.

"**Standard Contractual Clauses**" means the agreement executed between Customer and Company and attached hereto as Annex 2 pursuant to the European Commission's decision on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Subprocessor**" means any person (including any third party, but excluding an employee of Company or any of its sub-contractors) appointed by or on behalf of Company to Process Customer Personal Data on behalf of any Customer Group Member in connection with the Agreement.

The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

Applicability; Processing of Customer Personal Data

This DPA applies only to the extent and as of the time that the Data Protection laws apply to Customer Personal Data and the Processing of such Customer Personal Data by a Contracted Processor under the Agreement.

Roles of the Parties: The parties acknowledge and agree that as between the Parties and with regard to the Processing of Customer Personal Data, Customer is the Data Controller, Company is a Data Processor, and Company will engage Subprocessors only pursuant to the requirements set forth in Section 5; provided, however, that in the event, and to the extent, that Customer may be acting as a Processor for a third-party Controller, then Company shall be considered a Subprocessor under the Standard Contractual Clauses, to the extent applicable, with the same obligations as are imposed on the "data importer" thereunder, as described in Clause 11 of the Standard Contractual Clauses.

The objective of Processing of Customer Personal Data by Company is the performance of the Services pursuant to the Agreement. Certain details regarding the Contracted Processors' Processing of Customer Personal Data are set forth on Annex 1.

Each Customer Group Member instructs Company (and authorizes Company to instruct each Subprocessor) to Process Customer Personal Data and transfer Customer Personal Data to the United States (or any other country or territory specified by such Customer Group Member) for the following purposes: (i) Processing in accordance with the Agreement and applicable purchase order or similar document, (ii) Processing initiated by Customer and its authorized users, (iii) Processing to comply with other reasonable instructions provided by Customer, in each case consistent with the terms of the Agreement and applicable Data Protection Laws.

Each Customer Group Member giving any Processing instructions to Company represents and warrants that such instructions comply with Data Protection Laws and that it is and will at all relevant times remain duly and effectively authorised to give such instruction.

Each Customer Group Member, in its use of the Services, shall Process Customer Personal Data in accordance with Data Protection Laws and shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which such Customer Group Member acquired such Customer Personal Data.

Company shall not Process Customer Personal Data other than on the relevant Customer Group Member's documented instructions, including the instructions set forth above.

Subprocessing

Each Customer Group Member authorises Company to appoint (and permit each Subprocessor appointed in accordance with this Section to appoint) Subprocessors in accordance with this Section and any restrictions in the Agreement.

Company may continue to use those Subprocessors already engaged by Company as at the date of this DPA, as identified on Annex 3. Not all Subprocessors are used in connection with

every customer of Company. Personal Data of customers deployed in private cloud environments, for example, are not hosted or processed at Company's hosting services provider.

Company shall give Customer prior written notice of the appointment of any new Subprocessor, including details of the Processing to be undertaken by the Subprocessor. If, within ten (10) business days of receipt of that notice, Customer notifies Company in writing of any objections (on reasonable grounds) to the proposed appointment: Company shall take reasonable steps to address the objections raised by Customer, which may include making a change in the Services or recommending a commercially reasonable change in Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Company is unable to make any applicable change within a reasonable period of time, not to exceed sixty (60)] days, then, notwithstanding anything in the Agreement, Customer may by written notice to Company terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.

With respect to each Subprocessor, Company shall:

ensure that the arrangement with Subprocessor is governed by a written contract including terms which offer at least the same level of protection in connection with Restricted Transfers as those set out in this DPA; and

ensure that a legal basis for such Restricted Transfer as set forth in this DPA is incorporated into the agreement between Company and the Subprocessor, or before the Subprocessor first Processes Customer Personal Data procure that it enters into an agreement with Customer or the applicable Customer Group Member(s) to establish such legal basis.

Data Protection Impact Assessment and Prior Consultation

Company shall provide reasonable assistance to each Customer Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member under Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors. To the extent legally permitted, Customer shall be responsible for any costs arising from Company's provision of such assistance

Audit rights

Subject to the confidentiality obligations set forth in the Agreement or separately executed confidentiality agreement, if any, Company shall make available to Customer on request information regarding Company's compliance with this DPA. Such information may include one or more reports generated by external, independent mechanisms to verify or certify the adequacy of Company's security measures, including, as applicable, a System and Organization Controls (SOC) report, an appropriate International Organization for Standardization (ISO) certification, a Shared Assessments Standardized Information Gathering (SIG) form or Standardized Control Assessment (SCA) report, or a comparable, industry-standard report or certification (each, a "**Report**"). At Customer's written request, Company will provide Customer with its then-current Report, if applicable, or a summary thereof, so that Customer can reasonably verify Company's compliance with the security obligations under this DPA. Each Report and summary thereof constitutes Company's Confidential Information under the confidentiality provisions of the Agreement or separately executed confidentiality agreement, as applicable.

If the Standard Contractual Clauses apply, the Customer agrees to exercise its audit right by instructing Company to deliver the Report as described above. If Customer exercises its right to change the foregoing instruction, then (a) before the commencement of any audit undertaken pursuant to such change, Customer and Company shall mutually agree upon the scope, timing, and duration of the audit, (b) Customer shall reimburse Company for any time expended for the audit, at Company's then-current professional services rates, which shall in any event be reasonable, (c) Customer shall promptly notify Company with information regarding any non-compliance discovered during the course of the audit, and (d) Customer shall comply (and ensure that its auditor complies) with Company's safety and security

policies and shall in any event avoid causing any damage, injury or disruption to Company's premises, equipment, personnel and business in the course of such an audit.

Restricted Transfers

If and when Company has certified to the U.S. Department of Commerce that Company complies with the Privacy Shield, Company will comply with the Privacy Shield regarding any Restricted Transfer and the subsequent Processing of Personal Data in connection with the Services. Such self-certification shall apply to such Restricted Transfers and Processing to the fullest extent permitted by the Data Privacy Laws.

Solely to the extent Section 6.1 does not apply to any Restricted Transfer due to the unavailability of the Privacy Shield or termination of such self-certification, each Customer Group Member (as "data exporter") and Company (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Customer Group Member to Company permitted under the Agreement.

The Standard Contractual Clauses shall come into effect under hereunder on the later of (i) the data exporter becoming a party to them; (ii) the data importer becoming a party to them; and (iii) commencement of the relevant Restricted Transfer.

Section 6.2 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

General Terms

Governing law and jurisdiction

Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

Nothing in this DPA reduces Company's or Customer's (or Customer User's) obligations under the Agreement in relation to the protection of Customer Personal Data or permits any party to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Privacy Shield or Standard Contractual Clauses, as applicable pursuant to Section 6, the Privacy Shield or Standard Contractual Clauses, as applicable, shall prevail.

Changes in Data Protection Laws, etc.

Customer may propose variations to the Standard Contractual Clauses if and as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which Customer in good faith believes are required as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law.

If Customer makes a proposal under Section 7.3, the parties shall work together in good faith to implement mutually-agreed changes, and Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Company to protect the Contracted Processors against additional risks associated with such changes.

Severance

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

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

[CUSTOMER]

Signature _____

Name _____

Title _____

Date Signed _____

APPNETA, INC.

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1 TO THE DPA:
DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

Subject matter and duration of the Processing of Customer Personal Data
The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this DPA and relate to network and application performance monitoring and reporting services.
The nature and purpose of the Processing of Customer Personal Data
The nature and purpose of the Processing of the Customer Personal Data are set out in the Agreement and this DPA and relate to network and application performance monitoring and reporting.
The types of Customer Personal Data to be Processed
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: IP addresses and, depending on the configuration decisions of Customer and its authorized users, usage data and/or user name or other user identifier.
The categories of Data Subject to whom the Customer Personal Data relates
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer its sole discretion, and which may include, but is not limited to the following categories of Data Subjects: Customer personnel and other users of networks and applications monitored as part of the Services.
The obligations and rights of Customer and Customer Affiliates
The obligations and rights of Customer and Customer Affiliates are set out in the Agreement and this DPA.

ANNEX 2 TO THE DPA: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: [*Customer*]
Address: []
Tel.: []; e-mail: []
Other information needed to identify the organisation: Not applicable.

(the data **exporter**)

And

Name of the data importing organisation: AppNeta, Inc.
Address: 285 Summer Street, 4th Floor, Boston, Massachusetts 02210, USA
Tel: +1-800-664-4402; e-mail: support@appneta.com
Other information needed to identify the organisation: Not applicable

(the data **importer**)

each a "party"; together "the parties",

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

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
(b) '*the data exporter'* means the controller who transfers the personal data;
(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised

disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

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

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
(e) that it will ensure compliance with the security measures;
(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
(d) that it will promptly notify the data exporter about:
(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
(ii) any accidental or unauthorised access, and
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
(b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.
Clause 8
Cooperation with supervisory authorities
1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

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 (Customer):

Name (written out in full):
Position:
Address: As set forth above.
Other information necessary in order for the contract to be binding (if any): None.

Signature……

On behalf of the data importer (Company):

Name (written out in full):
Position:
Address: As set forth above.
Other information necessary in order for the contract to be binding (if any): None.

Signature……

Appendix 1 to the Standard Contractual Clauses

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

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

Data exporter
The Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter, a provider of [*briefly describe Customer's business*].

Data importer
The Data Importer is the legal entity that has executed the Standard Contractual Clauses as Data Importer, a provider of network and application performance monitoring and reporting services.

Data subjects
The Data Subjects are described on Annex 1 to the Data Processing Addendum to which the Standard Contractual Clauses are attached as Annex 2.

Categories of data
The Categories of Data are described on Annex 1 to the Data Processing Addendum to which the Standard Contractual Clauses are attached as Annex 2.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: Not applicable.

Processing operations
The nature and purpose Processing of Personal Data by Data Importer are described on Annex 1 to the Data Processing Addendum to which the Standard Contractual Clauses are attached as Annex 2.

DATA EXPORTER (CUSTOMER)

Name:……
Authorised Signature ……

DATA IMPORTER (COMPANY)

Name:……
Authorised Signature ……

Appendix 2 to the Standard Contractual Clauses

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

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

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Importer has in relation to the Customer Personal Data implemented and shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These include safeguards for protection of the security, confidentiality, and integrity of Customer Personal Data, including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, alteration, disclosure or access of or to Customer Personal Data. Data Importer will not materially decrease the overall security of the Services during the term of the Agreement.

Such safeguards include, without limitation and as appropriate:

The measures described in the Security section of the Data Importer's website, addressing, in particular:

- pseudonymisation and/or encryption of Customer Personal Data
- ability to ensure ongoing confidentiality, integrity, availability and resilience of Processing systems and services
- process for regularly testing, assessing and evaluating security measures

The foregoing technical and organizational security measures are subject to technical progress and development, and Data Importer may implement adequate alternative measures. Material changes to such technical and organizational measures shall be documented.

- *Payment Cards*.

To the extent (if any) that Company Processes payment card data, Company shall adhere to and maintain, or in the case of using subcontractors Company will ensure such subcontractors adhere to and maintain, PCI DSS compliance.

- *Standards and Certifications*.

To the extent that Company is certified to the following standards and controls, Company shall adhere to and maintain, or in the case of utilizing subcontractors Company will ensure such subcontractors are certified by a third-party quality assessor and will adhere to and maintain, the following:

- Statement on Standards for Attestation Engagements (SSAE) No. 16 Type 2 report for all storage locations within the U.S.A., and International Standard for Assurance Engagements (ISAE) No. 3402 for all storage locations outside the U.S.A.; and
- International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 (ISO/IEC 27001:2013) controls.

Where Company is certified to the above-referenced standards and controls, it shall maintain its third-party certifications and conduct annual audits in accordance with those standards throughout the term of the Agreement.

- *Pseudonymization and Encryption*.

Where applicable, Company shall ensure pseudonymization and encryption of Personal Data.

- *Processing Systems*.

Company shall ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services.

- *Risk Assessments*.

Company shall conduct periodic risks assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of records containing Personal Data and develop a process for regularly testing, assessing and evaluating the effectiveness of its technical, administrative and organizational measures to ensure the security of the Processing and to limit any internal and external risks.

DATA EXPORTER (CUSTOMER)

Name:……
Authorised Signature ……

DATA IMPORTER (COMPANY)

Name:……
Authorised Signature ……

ANNEX 3 TO THE DPA: APPROVED SUBPROCESSORS

Amazon Web Services, Inc.

Google, LLC (BigQuery)