FAQ for Tealium’s Data Processing Addendum

This FAQ is designed to provide you with helpful information about Tealium’s privacy commitments regarding its Software as a Service offerings, taking into account the Parties’ role in the use and administration of the Services. This FAQ is provided for informational purposes only and will not form part of the contract being contemplated between the parties

Why do we need a Data Processing Addendum and what does it cover?
This Data Processing Addendum (“DPA”) forms part of the agreement covering your purchase of Services and covers all personal data you upload to our cloud based multi-tenant or private cloud data warehouse solution (defined as “Services” in the master agreement). We do not have visibility to the data our customers upload to our Services, which is why we enter into our DPA with all of our customers. Our DPA reflects our privacy program for data we process in the Services and addresses certain obligations each respective party has under applicable data protection laws. Our DPA also addresses additional requirements of the European Union’s Regulation 2016/679 (“GDPR”), the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (“CCPA”), and the Australian Privacy Act 1988 (Cth.).

Why do we need to use the Tealium DPA instead of our own data processing addendum?
There are specific reasons why we offer a DPA instead of using the data processing addendums of customers.

1. The Services is provided to our customers using a “one-for-all” model, meaning the same Services is provided to all of our customers. We do not offer a “customized” service offering that would allow us to treat one customer (or its data), differently from other customers. Even our ancillary services (such as deployment or support) are provided in a uniform manner across our customer base. While there is no customized offering, you are able to select the particular geographic hosting location(s) for your account, as further defined in the DPA.

2. Tealium requires that you encrypt personal data before you transmit data to us and as such we do not have access to unencrypted data. As set out in our Data Security Statement, we do not access unencrypted data you upload to our Service, unless you grant us access for a particular purpose (e.g., a support request). If you choose to grant us access, you control the access permissions and can terminate our access at any time.

3. Tealium has no visibility into the content of a customer’s data. Because we do not access unencrypted data as described above, we do not have visibility to the nature of the data (including whether or not it is pseudonymized, personal or sensitive), the particular manner in which you store or structure that data in your account, to whom the data relates, the purposes for which you process the data, the scope/volume of your processing, third parties you transmit the data to, and whether (or the degree to which) the particular data and/or processing poses risks to data subjects. Due to the foregoing, we will also not have visibility necessary to determine which portions of the data may be subject to industry-specific or country-specific regulations.

4. All customers benefit uniformly from Tealium’s uniform and rigorous security controls. Because the same Service is provided to all customers, you benefit from a set of shared technical and organizational security measures. Services provided in our private cloud environment have enhanced technical and organizational security measures such as an attestation of compliance with the US HIPAA regulations.

Does Tealium have technical and organizational security measures in place that are designed to protect Customer Data?
Tealium’s security measures are detailed in Tealium’s data security statement or DSS.

Does the DPA address article GDPR's 28(3) requirements?
We drafted our DPA specifically to satisfy the requirements of GDPR, including those of Article 28(3). Because we do not have access or visibility to your data, you play an important role in how some of the requirements of GDPR are satisfied. For example, we are transparent about the comprehensive technical and organizational measures we implement, including the many audits and certifications we undergo and make available to you, but ultimately you play an indispensable role in determining whether the Services is appropriate for your specific use case and whether or not our Services meets requirements applicable to your particular data.

Does the DPA address the CCPA?
The DPA addresses the requirements of the CCPA. Tealium acts as a Service Provider as that term is defined in the CCPA. Section 2 of the DPA specifies that Tealium does not sell your data, or use or otherwise transmit your data except as instructed by you. However, as stated previously, Tealium does not have access or visibility to your data, and you play an important role in how some of the requirements of CCPA are satisfied. For example, we are transparent about the comprehensive technical and organizational measures we implement, including the many audits and certifications we undergo and make available to you, but ultimately you play an indispensable role in determining whether the Services is appropriate for your specific use case and whether or not our Services meets requirements applicable to your particular data.

TEALIUM INC. DATA PROCESSING ADDENDUM
(Addendum DPA-1)

This Data Processing Addendum (“DPA”) forms part of, and is subject to, the Master Services Agreement or other written or electronic terms of service or subscription agreement between Tealium and Customer for Customer’s purchase of Services from Tealium that references this DPA (the “MSA”).

1. Definitions. For the purposes of this DPA, the terminology and definitions as used by the GDPR and the CCPA (as defined herein) shall apply. In addition, unless otherwise defined in the MSA, all capitalized terms used in this DPA will have the meanings given to them below:

“AWS” means Amazon Web Services, Inc.

“CCPA” means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.

“Data Exporter” and **“Data Importer”** have the meanings given them in the Standard Contractual Clauses.

“Data Protection Laws and Regulations” means all laws and regulations applicable to each respective Party in its role in the Processing of Personal Data under the MSA, including where applicable, the GDPR, the Privacy Act, and the CCPA.

“Data Security Statement” or **“DSS”** means Tealium’s statement of its technical and organizational security measures.

“EEA” means, for the purpose of this DPA, the European Economic Area and the UK.

“GDPR” means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Highly Sensitive Data” means personal data whose unauthorized disclosure or use could reasonably entail a serious potential security or privacy risk for a data subject, including but not limited to government issued identification numbers such as national insurance numbers, passport numbers, driver’s license numbers, or similar identifier, or credit or debit card numbers, medical or financial information, biometric data, and/or financial, medical or other account authentication data, such as passwords or PINs.

“Personal Data” has the meaning set forth in Data Protection Laws and Regulations relating to the collection, use, storage or disclosure of information about an identifiable individual, or if no definition, means information about an individual that can be used to identify, contact or locate a specific individual, or can be combined with other information that is linked to a specific individual to identify, contact or locate a specific individual. For purposes of the DPA, Personal Data is as described in the scope of Processing described in Appendix 1.

“Privacy Act” means the Australian Privacy Act 1988 (Cth.).

“Processing” or **“Process”** means any operation or set of operations which is performed on Personal 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.

“Service Provider” shall have the meaning set forth in the CCPA.

“Standard Contractual Clauses” means Annex 1 attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data, but does not include any Unsuccessful Security Incident.

“Tealium Network” means the data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within the control of Tealium or its sub-processors and are used to provide the Services.

“Unsuccessful Security Incident” means an unsuccessful attempt or activity that does not compromise the security of Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

“User Data” means the login details and contact information of the authorized users of the Services and will be deemed Personal Data.

Further definitions are provided throughout this DPA.

2. Data Processing.

2.1 Scope and Roles. This DPA applies where and only to the extent that Tealium Processes Personal Data on behalf of Customer as a data processor or Service Provider in the course of providing Services pursuant to the MSA. Tealium will engage sub-processors pursuant to the requirements for subcontractors set forth in Section 10 below.

2.2 Compliance with Laws. Each party will comply with all Data Protection Laws and Regulations applicable to it and binding on it in the provision or receipt of Services under the MSA, including all statutory requirements relating to data protection.

2.3 Customer Processing of Personal Data. Customer agrees that: (a) it has provided all notices and obtained all consents, permissions and rights necessary under Data Protection Laws and Regulations for Tealium to lawfully process Personal Data; (b) Customer will not transmit to Tealium nor require Tealium to process any Highly Sensitive Data; and (c) Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.4 Instructions for Data Processing.

2.4.1 Tealium will Process Personal Data on behalf of and only in accordance with Customer’s documented instructions, including with regard to transfers of Personal Data to a third country or an international organization, unless otherwise required by Data Protection Laws and Regulations to which Tealium is subject; in such a case, Tealium shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Tealium will not sell Personal Data.

2.4.2 Customer instructs Tealium to process Personal Data for the following purposes: (a) processing in accordance with the MSA; (b) processing in accordance with this DPA; and (c) processing to comply with any reasonable written request from Customer that are consistent with the terms of the MSA and this DPA. In particular Tealium will retain, use or disclose Personal Data only for the specific purpose of performing the Services. By entering into this DPA, Tealium certifies that it understands its contractual restrictions and shall comply with them. Processing outside the scope of this Section 2.4 (if any) will require prior written agreement between Tealium and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to Tealium for carrying out such instructions.

2.4.3 Customer shall ensure its processing instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws and Regulations or cause Tealium to be in breach of Data Protection Laws and Regulations. Tealium shall immediately inform Customer if, in its opinion, an instruction infringes any provision of Data Protection Laws and Regulations. In such case, Tealium is not obliged to follow the instruction unless and until Customer has confirmed or changed such instruction.

2.5 Disclosure. Tealium will not disclose Personal Data to any third party other than as expressly permitted by the terms of the MSA, and except as necessary to comply with applicable laws and regulations or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Tealium a demand for Personal Data, Tealium will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Tealium may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then Tealium will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Tealium is legally prohibited from doing so.

3. Tealium Personnel.

3.1 Confidentiality, Reliability, and Limitation of Access. Tealium will ensure that its personnel authorized to Process Personal Data have committed themselves to appropriate contractual obligations, including relevant obligations regarding confidentiality, data protection and data security, or are under an appropriate statutory obligation of confidentiality. Tealium will take reasonable steps to ensure the reliability of Tealium personnel engaged in the Processing of Personal Data. Tealium restricts its personnel from Processing Personal Data without authorization by Tealium as described in the Data Security Statement.

3.2 Training. Tealium will ensure that its personnel have received appropriate training on their responsibilities concerning Personal Data.

3.3 Data Protection Officer. Tealium has appointed a data protection officer. The appointed person can be reached at dpo@tealium.com.

4. Other obligations of Tealium. Tealium will:

4.1 take 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, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk. Such measures shall, at a minimum, meet the specifications set forth in the Data Security Statement;

4.2 respect the conditions referred to in Section 10 of this DPA for engaging a sub-processor;

4.3 take into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to requests regarding data subject rights under Data Protection Laws and Regulations as described in Section 5 of this DPA;

4.4 take into account the nature of processing and the information available to Tealium, assist Customer in ensuring compliance with its obligations under Data Protections Laws and Regulations with regard to security of processing, data breach notification, conducting privacy impact assessments and cooperation with supervisory authorities.

5. Customer Controls and Data Subject rights.

5.1 Customer Controls. The Services provide Customer with controls to enable Customer to retrieve, correct, delete, or block Personal Data and to respond to Data Subject Requests as defined below. Tealium makes available certain security features and functionalities that Customer may elect to use. Customer is responsible for properly (a) configuring the Services, (b) using the controls available in connection with the Services (including the security controls), and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, deletion and backup of Personal Data, which may include use of encryption technology to protect Personal Data from unauthorized access and routine archiving of Personal Data.

5.2 Data Subject Rights. Tealium shall, to the extent legally permitted, promptly notify Customer if Tealium receives a request from a data subject known to Tealium to be associated with Customer, to exercise the data subject's right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, object to the processing, or its right not to be subject to an automated individual decision making (**"Data Subject Request"**). In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Tealium will upon Customer's request provide assistance to Customer in responding to such Data Subject Request, to the extent Tealium is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations.

6. Transfers of Personal Data.

6.1 Regions. Customer may specify the location(s) where Personal Data, not including User Data, will be hosted within the Tealium Network from the following list, as updated by Tealium from time to time: (i) California, USA; (ii) Virginia, USA; (iii) Dublin, Ireland; (iv) Frankfurt, Germany; (v) Tokyo, Japan; and (vi) Sydney, Australia (each a **"Region"**). Once Customer has made its choice, by properly configuring the Services, Tealium will not transfer the hosting of Personal Data from Customer's selected Region(s) except under Customer's further instructions or as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order) as described in Section 2.5. User Data will be hosted in California, USA in all cases.

6.2 Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data; and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply: (x) if Tealium is acting as a sub-processor (as defined in the Standard Contractual Clauses) with respect to Personal Data, (y) if Tealium has adopted Binding Corporate Rules, or (z) if Tealium has adopted an alternative recognized compliance standard for the lawful transfer of personal data outside the EEA in accordance with Article 46 of the GDPR.

7. Security Responsibilities of Tealium.

7.1 Continued Evaluation. In addition to its obligations under Section 4.1 of this DPA, Tealium will conduct periodic reviews of the security of its infrastructure, applications, and associated Services. The adequacy of Tealium's information security program is measured against industry security standards and compliance with Tealium's policies and procedures. Tealium will continually evaluate the security of the Tealium Network and associated Services to determine whether additional or mitigating security measures are required to respond to new security risks or findings generated by the periodic reviews. Tealium conducts ongoing vulnerability scans and annual penetration tests to identify and then remediate identified deficiencies. The Tealium Network and associated Services are continuously monitored for events and potential Security Incidents. Tealium also conducts risk assessments at least annually or when significant changes to the environment occur. These activities provide for a continually improving information security program.

7.2 Customer Independent Review. Customer is solely responsible for reviewing the information made available by Tealium relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security**.**

8. Certifications and Audits.

8.1 Tealium Audits. Tealium audits its security measures at least annually. These audits: will be performed according to ISO 27001, ISO 27018 and SOC 2 Type II standards or such other alternative standards that are substantially equivalent to such standards. These audits will be performed by independent third party security professionals at Tealium's selection and expense.

8.2 Audit Reports. At Customer's written request, Tealium will provide Customer with a confidential report so that Customer can reasonably verify Tealium's compliance with its obligations under this DPA. The report constitutes Tealium's Confidential Information.

8.3 AWS and Customer Audits. Customer audits rights are as set forth in the DSS.

9. Security Incident Notification.

9.1 Tealium Notification. If Tealium becomes aware of a Security Incident, Tealium will without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify Customer of the Security Incident. Where the notification to the Customer is not made within 48 hours, it shall be accompanied by reasons for the delay.

9.2 The notification referred to in Section 9.1 shall at least:

9.2.1 describe the nature of the Security Incident;

9.2.2 communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

9.2.3 describe the measures taken or proposed to be taken by Tealium to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9.4 Tealium shall document any Security Incidents, comprising the facts relating to the Security Incident, its effects and the remedial action taken. That documentation shall enable Customer to verify compliance with this Section.

9.5 Tealium Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under the Data Protection Laws and Regulations, Tealium will include in the notification under section 9.1 such information about the Security Incident as Tealium is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Tealium, and any restrictions on disclosing the information, such as confidentiality.

9.6 Limitations. Customer agrees that:

9.6.1 An Unsuccessful Security Incident will not be subject to this Section; and

9.6.2 Tealium's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Tealium of any fault or liability of Tealium with respect to the Security Incident.

9.7 Delivery. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any reasonable means Tealium selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information with Tealium all times.

10. Sub-Processing.

10.1 Authorized Sub-processors. Customer agrees that Tealium may use AWS as a sub-processor to fulfill certain of its contractual obligations under this DPA or to provide certain services on its behalf. Tealium will inform Customer of any intended changes concerning the addition or replacement of sub-processors, thereby giving Customer the opportunity to object to such changes.

10.2 Obligations in respect of sub-processors. Where Tealium authorizes any sub-processor as described in this Section 10:

10.2.1 Tealium will restrict the sub-processor's access to Personal Data only to what is necessary to maintain the Services or to provide the Services to Customer and Tealium will prohibit the sub-processor from accessing Personal Data for any other purpose;

10.2.2 Tealium will impose appropriate contractual obligations in writing upon the sub-processor that are no less protective than this DPA, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and

10.2.3 Tealium will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processor that cause Tealium to breach any of Tealium's obligations under this DPA.

10.3 Objection to Sub-Processor. If Customer has a reasonable basis to object to Tealium's use of a new sub-processor, Customer shall notify Tealium promptly in writing within ten (10) business days after receipt of Tealium's notice. If Customer objects to a new sub-processor(s) Tealium will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid Processing of Personal Data by the objected-to new sub-processor without unreasonably burdening Customer. If Tealium is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Service Order in respect only to those Services that cannot be provided by Tealium without the use of the objected-to new sub-processor, by providing written notice to Tealium. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

11. Duties to Inform. If Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Tealium, Tealium will inform Customer without undue delay. Tealium will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Personal Data subjected to those proceedings is Customer's property and area of responsibility and that Personal Data is at Customer's sole disposition.

12. Termination of the DPA. This DPA shall continue in force until the termination of the MSA (the "Termination Date").

13. Return and Deletion of Customer Personal Data. The Services provide Customer with controls that Customer may use to retrieve or delete Personal Data. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete Personal Data in accordance with this Section. To the extent Customer is unable to retrieve or delete Personal Data itself through its use of the Services, Tealium will assist Customer in such retrieval or deletion upon Customer's written request. Tealium will delete Personal Data within 180 days following the Termination Date.

14. Additional Terms for EEA Personal Data. Where the Standard Contractual Clauses in Annex 1 apply to the Processing of Personal Data by Tealium in the course of providing the Services the additional terms in this Section 14 will also apply. For the avoidance of doubt, the following terms are provided for clarification only. Nothing in this Section 14 varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

14.1 The parties agree that the copies of the sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand; and, that such copies will be provided by Data Importer only upon reasonable written request by Data Exporter.

14.2 The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Data Exporter may contact Data Importer in accordance with the "Notices" Section of the MSA to request an on-site audit of the procedures relevant to the protection of personal data. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration of the audit. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit. With respect to the AWS component of the Tealium Network, Customer audit right is as described in the DSS.

14.3 The parties agree that the certification of deletion of personal data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's written request.

15. Fees and Expenses. To the extent legally permitted, Customer shall be responsible for any costs and fees arising from a request by Customer to change the Region originally chosen by Customer during configuration of its account(s) pursuant to Section 6.1 above.

16. Nondisclosure. Customer agrees that the details of this DPA are not publicly known and constitute Tealium's Confidential Information under the confidentiality provisions of the MSA.

17. Conflict. Except as amended by this DPA, the MSA will remain in full force and effect. If there is a conflict between the MSA and this DPA, the terms of this DPA will control.

18. Counterparts; Electronic Signature or Email Delivery. This DPA may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this DPA by electronic signature or email transmission.

Accepted and agreed as of the Effective Date by the authorized representative of each party:

"Tealium" TEALIUM INC.	**"Customer"**
Signature: Doug Lindroth Doug Lindroth (May 8, 2020)	Signature:________________
Printed Name: Doug Lindroth	Printed Name:________________
Title: CFO	Title: ________________
Date: May 8, 2020	Date:________________

Annex 1

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

The entity identified as “Customer” in the DPA
(the “**data exporter**”)

and

Tealium Inc.
11095 Torreyana Road,
San Diego, CA 92121
(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

For the purposes of the Clauses:

1. Definitions

“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;

“the data exporter” means the controller who transfers the personal data;

“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;

“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;

“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;

“technical and organizational security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

1. 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;

2. 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;

3. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

4. 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;

5. that it will ensure compliance with the security measures;

6. 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;

7. 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;

8. 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;

9. 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

10. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The data importer agrees and warrants:

1. 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;

2. 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;

3. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

4. that it will promptly notify the data exporter about:

1.1 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,

1.2 any accidental or unauthorized access, and

1.3 any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

5. 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;

6. 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;

7. 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;

8. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;

10. 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:

1.1 to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

1.2 to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case, the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter

Name (written out in full): ……………………………………………………………….………………....

Position: ………………………………………………………………………………………….…………..

Address: ……………………………………………………………………….……….……….…………..

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

(Stamp of organization)

Signature: …………………………………..

On behalf of the data importer

Name (written out in full): Doug Lindroth

Position: Chief Financial Officer

Address:
11095 Torreyana Road,
San Diego, CA 92121

Other information necessary in order for the contract to be binding (if any):
None

Signature: Doug Lindroth
Doug Lindroth (May 8, 2020)…………………...
(Stamp of organization)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 1 to the Standard Contractual Clauses 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 (please specify briefly your activities relevant to the transfer) the legal entity that has executed the Standard Contractual Clauses.

Data importer.

The data importer is (please specify briefly activities relevant to the transfer):

Tealium Inc., a provider of web services

Data subjects.

The personal data transferred concern the following categories of data subjects (please specify): Data exporter may submit personal data to the Tealium Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and may include personal data relating to the following classes of data subjects: (a) website, mobile or other visitors to data exporter's digital or physical properties; and (b) data exporter's employees or agents who are users of the Services.

Categories of data

The personal data transferred concern the following categories of data (please specify): Data exporter may submit personal data regarding the data subjects stated above to the Tealium Services, the extent of which is determined and controlled by the data exporter in its sole discretion.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): Data exporter determines and controls the scope of personal data Processed subject to limitations in the MSA, including prohibition on processing Highly Sensitive Data.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify) and purposes: The processing activities and the purpose of the Processing of personal data by data importer is the performance of the Tealium Services pursuant to the MSA.

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):
………

(Stamp of organization)

Signature: ……………………………………...

On behalf of the data importer

Name (written out in full): Doug Lindroth

Position: Chief Financial Officer

Address:
11095 Torreyana Road,
San Diego, CA 92121

Other information necessary in order for the contract to be binding (if any):
None

Signature: Doug Lindroth
Doug Lindroth (May 8, 2020)…………………..
(Stamp of organization)

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) (or document/legislation attached):

The technical and organizational security measures implemented by the data importer are as described in Tealium's Data Security Statement**.**