FAQ for Tealium's Customer Protection Package ("CPP")

Thank you for taking the time to review this FAQ. It was designed to provide you with helpful information about Tealium's Customer Protection Package, which includes the documents that describe the protections and commitments that Tealium offers all its customers. This FAQ is provided for informational purposes only and will not form part of the contract being contemplated between the parties. Note, all liability issues for the DSS and DPA are addressed in the MSA.

What is the structure of the CPP?

Our CPP is made up of three documents:
The **Service Level Agreement ("SLA")** contains our commitment to availability across all our Services, and your remedies in the unlikely event we do not meet our commitment.

The **Data Security Statement ("DSS")** contains details of the organizational and technical security measures designed to protect your data.

The **Data Processing Agreement ("DPA")** contains details of our data processing commitments in compliance with applicable privacy laws and regulations.

SLA

Tealium has a website that provides real-time status, as well as notifications for maintenance and emergency outages. This can be found at https://status.tealium.com. We provide remedies in the unlikely event that we miss the availability commitments in the SLA, as well as a termination right for chronic outages. Since our SLA is being provided across all our products, and we are delivering a multi-tenant SaaS service, we are unable to alter our SLA for any single customer. We are confident that our SLA is industry standard and will address all our customers' issues.

DSS

Why do we need a Data Security Statement and what does it cover?

The DSS forms part of the agreement covering your purchase of the Services and all electronic data and information submitted by or for you to the Services, including enhancement and output derived from the use of the Services ("Customer Data"). Our DSS reflects Tealium's security policies and procedures for Customer Data, which apply to all our customers equally.

How does Tealium protect personal data submitted to the Services?

Details of the data privacy program and the measures Tealium has in place to protect Personal Data are set forth in our Data Processing Addendum ("DPA").

Why do we need to use the Tealium DSS instead of our own data security documentation?

There are specific reasons why we offer a DSS instead of using the data security addendums provided by our customers.

The Services are provided to our customers using a "one-for-all" model, meaning the same Services are provided to all our customers. We do not offer a "customized" service offering that would allow us to treat one customer (or its Customer Data) differently from other customers.

We do not access your Customer Data, unless you instruct us to do so for a particular purpose (e.g., a

support request) or as otherwise permitted by the MSA. If you instruct us to access your Customer Data, you control the access permissions and can terminate our access at any time.

As such, we do not control any of the following with respect to your Customer Data:

- The nature of the data, including, but not limited to, whether the data 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;
- 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.

Our Services are industry-agnostic, therefore, we cannot determine which portions of the data may be subject to country and/or industry-specific regulations.

All of our customers benefit uniformly from Tealium's rigorous security controls. Because the same Services are provided to all customers, you benefit from a set of shared technical and organizational security measures.

Does the DSS address legal requirements?
You play an important role in how legal requirements pertaining to your Customer Data 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 are appropriate for your specific use case and whether or not the Services meet your security and legal requirements applicable to your particular Customer Data.

Does Tealium have a mechanism to allow customers to easily find additional information about Tealium's TOMS?

Yes, Tealium's security measures are detailed at trust.tealium.com (the "**Trust Center**").

DPA

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 (as defined in the DPA) that is included in Customer Data. Tealium acts as a data processor or service provider for the Personal Data that our customers submit to the Services. Our DPA reflects our privacy program for Personal Data we process in the Services and addresses the obligations Tealium has under applicable data protection laws.

Tealium has customers that operate globally, so our DPA addresses data protection requirements globally, including the additional requirements of the European Union's Regulation 2016/679 ("**GDPR**"), US Privacy Laws, as defined in the DPA, the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), the Australian Privacy Act 1988 (Cth.), and the Japan Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020), as amended or supplemented from time to time.

Why do we need to use the Tealium DPA instead of customers' data processing addendums?
There are specific reasons why we need to use the Tealium DPA instead of using the data processing addendums of customers.

1. The Services are provided to our customers using a “one-for-all” model, meaning the same Services are provided to all of our customers. We do not offer a customized service offering that would allow us to treat one customer (or its Personal 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 configure the Services to your processing requirements and also select the particular geographic hosting location(s) for your account, as further defined in the DPA.

2. All our Services are industry-agnostic. Therefore, we cannot determine which portions of the Personal Data may be subject to industry-specific regulations. All customers benefit equally 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.

3. Our HIPAA Cloud Services have enhanced technical and organizational security measures in order to comply with the US HIPAA regulations. If you intend to send PHI to Tealium and you are purchasing HIPAA Cloud Services, please request a Business Associate Agreement from Tealium.

Does Tealium have technical and organizational security measures in place that are designed to protect Personal Data?

Yes, please see Tealium’s DSS (discussed in greater detail above).

Does the DPA address GDPR, including GDPR’s Article 28(3) requirements?
We drafted our DPA specifically to satisfy the requirements of GDPR, including those of Article 28(3). 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 must determine whether the Services are appropriate for your specific use case and whether or not our Services meet requirements applicable to your particular Personal Data.

Does the DPA address US Privacy Laws such as the CCPA (including the changes made by the CPRA)?
The DPA addresses the requirements of the CCPA as amended and updated by the CPRA. 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 or share your Personal Data. Tealium will not use or otherwise transmit your Personal Data except as instructed by you or as otherwise permitted by the MSA. As stated previously, 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 must determine whether the Services are appropriate for your specific use case and whether or not our Services meet requirements applicable to your particular data.

What about cross-border data transfers?
Where personal data is transferred from one region to another, Tealium will provide all information necessary for our customers to conduct transfer impact assessments in connection with their use of Tealium’s services. More detail on the assistance and safeguards provided by Tealium can be found here: https://tealium.com/data-transfer/ and in the Trust Center.

Service Level Agreement (SLA)

This Service Level Agreement ("SLA") is incorporated into, and made a part of, the Master Services Agreement ("MSA) and Service Order between Tealium Inc. and Customer that references this SLA.

1. Definitions. The following defined terms are used in this SLA:

"Available" or "Availability" means the Services are in an operable state, and the Service can be accessed through programmatic access (APIs, tags, HTTP requests/responses) or user interface access as applicable to the particular Service. Solely for Delivery Network performance, "Available" means Delivery Network servers are responding to requests for libraries.

"Delivery Network" means the content delivery network service providers used in connection with certain Services for the purpose of serving Tealium JavaScript or other Service related files ("Libraries") to Digital Properties.

"Force Majeure" means any cause beyond such Party's reasonable control, including but not limited to the weather, unavailability of utilities or communications services (including access to the Internet), civil disturbances, acts of civil or military authorities, or acts of God.

"Monthly Subscription Amount" means the contracted amount for the Services for the Service Term, divided by the number of months in the Service Term (excluding fees for implementation, managed, and professional services and Additional Usage Fees).

"Monthly Uptime Percentage" means the percentage of time within a given calendar month the Services are Available.

"Service Credit" means a credit, calculated as set forth below, that Tealium may credit towards future invoices to Customer.

2. Service Uptime Commitment. Tealium will use commercially reasonable efforts to make the Services available with a Monthly Uptime Percentage of at least 99.9% during any month (the "Service Commitment"). In the event the Services do not meet the Service Commitment, Customer will be eligible to receive a Service Credit as described below.

3. Service Credits. Service Credits are calculated as a percentage of the Monthly Subscription Amount for the specific Service for the month in which the Service Commitment for a particular Service was not met in accordance with the schedule below. Tealium will apply any Service Credits only against future payments. If Customer has prepaid in full for all Services under the MSA, in the event the MSA expires and is not renewed, Customer will be entitled to a refund of the Service Credit amount upon written request to Tealium. Customer's sole and exclusive remedy for any failure of the Services to meet the Service Commitment is the receipt of a Service Credit in accordance with the terms of this SLA. Service Credits may not be transferred or applied to any other Customer account.

Service Level (%)	Credit (%)
98-99.89	5
95-97.99	10
<95	15

4. Credit Request and Payment Procedures. To receive a Service Credit, Customer must submit a request by sending an e-mail message to services@tealium.com. To be eligible, the credit request must (a) include a reasonably detailed list of the instances of unavailability that together evidence Tealium's failure to meet Service Commitment in a given month; (b) include, in the body of the e-mail, the dates and

times of each incident that Customer claims to have experienced; (c) include Customer's additional information (e.g. server request logs) that document and enable Tealium to corroborate Customer's claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (d) be received by Tealium within ten (10) business days after the end of the month inwhich the Service Commitment was not met. In order for Credit to be awarded, Tealium must be able to independently verify the instances of unavailability reported by Customer pursuant to this Section 4.

5. SLA Exclusions. The Service Commitment does not apply to any Services unavailability or other performance issues: (a) caused by factors outside of Tealium's reasonable control, including any Force Majeure event or Internet access or related problems beyond the demarcation point of Tealium's network or the Delivery Network; (b) that result from any actions or inactions of Customer or any third party; (c) that result from Customer's equipment, software or other technology or third party equipment, software or other technology (other than third party equipment within Tealium's direct control); (d) arising from the suspension and termination of Customer's right to use a Service in accordance with the MSA; or (e) arising from scheduled downtime for system or network maintenance.

6. **Chronic Outage Termination Right**. In addition to the Service Credit remedies described in Section 3 above, if the monthly Uptime Percentage is less than 95% for two (2) consecutive months or any four (4) months in a rolling twelve (12) month period then Customer will have the right to terminate the Service Order for the adversely affected Services and receive a refund of any amounts paid in advance attributable to periods after the effective date of termination. In order for such termination to be effective, written notice of such termination must be received by Tealium with thirty (30) days following the month in which the right to termination arose.

7. Non-Tealium Products; Connectors. Upon notification that there is a Connector failure, either from Tealium's receipt of error messages from the Connectors, or from Customer, Tealium will commence investigating such Connector failure within five (5) business days. Where Tealium has created the Connector, Tealium will make commercially reasonable efforts to work with the third-party provider of the Connector to remedy the Connector failure and to implement any solution or patch provided by the third-party provider in a reasonably timely manner. Any issues under this Section are specifically excluded from the Availability.

DATA SECURITY STATEMENT (DSS)

This Data Security Statement ("DSS") is incorporated into, and made a part of, the MSA between Tealium and Customer.

1. General.

1.1. Tealium will implement and maintain administrative, logical, and physical security controls with respect to its Processing of Customer Data. These controls are designed to provide appropriate technical and organizational safeguards against the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or unauthorized access to, Customer Data at least equal to Industry Standards, but which in no event are less protective than the specific requirements of this DSS. Tealium will implement measures for ensuring ongoing confidentiality, integrity, availability, and resilience of the Tealium Services. Tealium will regularly re-evaluate and modify its security standards and controls as Industry Standards evolve, new technologies emerge, or new threats are identified. Unless otherwise agreed, all Customer Data Processing will be in a multi-tenant environment with logical segmentation controls.

1.2. Customer agrees that Tealium may use the Sub-processors set forth at https://tealium.com/subprocessors/ to fulfill certain portions of its contractual obligations under this DSS or to provide certain services on its behalf. Tealium will inform Customer at least 30 days in advance of any intended changes concerning the addition or replacement of Sub-processors, thereby giving Customer the opportunity to object to such changes, as outlined in the DPA.

2. Definitions.

"Dynamic Application Security Testing" or **"DAST"** means a security test of an application designed to detect conditions indicative of a security vulnerability in an application as it runs in a production environment, or in a test environment representative of the production environment in which such application will run.

"Encryption" means the process of using a cryptographic algorithm to transform data from plaintext to ciphertext in order to protect the confidentiality of the data.

"Firewall" means an integrated collection of security measures used to prevent unauthorized electronic access to the Tealium Systems by implementing predetermined security rules for network communication.

"Industry Standards" means customs and practices followed by, and representing the degree of skill, care, prudence and foresight expected from, providers of the types of services that are the subject matter of the MSA.

"Intrusion Detection System" or **"IDS"** means a method or system of reviewing system logs and processes in near real-time and escalating identified events or patterns of behavior that indicate an intrusion is occurring or is likely to occur soon without unreasonable delay.

"Least Privilege" means that every module in a particular computing environment (such as a process, a user, or a program) may only access the information and resources that are necessary for its legitimate purpose.

"Malicious Code" means computer instructions or software code whose purpose is to disrupt, damage or interfere with the Services or any Party's computer or communications systems, networks, facilities or equipment, or to provide unauthorized access to such systems, networks, facilities or equipment. Examples of Malicious Code include, without limitation, any code containing viruses, Trojan horses, worms, traps, spyware, back doors, disabling devices or similar destructive code or code that self-replicates.

"Multifactor Authentication" means authentication using at least two of the following factors: "something you know" such as a password, "something you have" such as a token, or "something you are" such as a biometric reading.

"Penetration Testing" or **"PenTest"** means a manual and/or automated security test of an application, executed by a combination of automated tools, a qualified tester, and/or a qualified third-party.

"Processing" or **"Process"** means any operation or set of operations that is performed on Customer Data, whether or not by automated means, such as viewing, 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.

"Removable Media" means any portable or removable external data storage device.

"SDLC" means secure software development lifecycle methodology, a documented process for planning, creating, testing, and deploying, and/or delivering, an information system that requires information security engagement, particularly with respect to the design, build, test, and deployment stages.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, but does not include any Unsuccessful Security Incident.

"Separation of Duties" means dividing roles and responsibilities so that a single individual cannot subvert the security controls of a critical process.

"Software Composition Analysis" or **"SCA"** means a security test to identify any known security vulnerabilities in any open source and/or third party libraries included in a codebase.

"Static Application Security Test" or "SAST" means a security test of an application's source code designed to detect conditions indicative of a security vulnerability in an application's code.

"Sub-processor" means a processor who is engaged by Tealium to carry out specific processing activities on Customer Data on behalf of Tealium.

"Tealium Systems" means the data centers, servers, networks, networking equipment, applications, 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.

"Threat Model" means identifying, communicating, and understanding threats and mitigations within the context of protecting something of value.

"Trust Center" means Tealium's compliance documentation repository located at trust.tealium.com. The Trust Center is a self-service repository of Tealium's compliance documentation, such as policies, automated monitoring data, and information regarding Sub-processors.

"Unsuccessful Security Incident" means an unsuccessful attempt or activity that does not compromise the security of Customer Data, including (without limitation) pings and other broadcast attacks on 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 to Customer Data) or similar incidents.

"Root Cause Analysis" means a principle-based, systems approach for the identification of the underlying causes associated with a Security Incident.

3. Incident Management and Security Incident Notification.

3.1. Incident Management. Tealium maintains a documented incident management policy and process to detect Security Incidents, which provides coordinated response to threats and Customer notification.

3.2. Security Incident Notification & Remediation. In the event of a Security Incident, Tealium will notify Customer and remediate the Security Incident in the manner set forth below:

3.2.1. Notification. Tealium will without undue delay and, where feasible, no later than 48 hours after having become aware of it, notify Customer of the Security Incident. Where the notification to Customer is not made within 48 hours, it shall be accompanied by reasons for the delay.

The notification shall at least:

(1) describe the nature of the Security Incident;

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

(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.

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.

Tealium shall document any Security Incidents, comprising the facts relating to the Security Incident, its effects, and the remedial action taken.

3.2.2. Root Cause Analysis. Tealium will promptly initiate and pursue to completion a Root Cause Analysis without undue delay.

3.2.3. Remediation. Tealium will promptly implement measures necessary to restore the security of Customer Data and Tealium Systems. If such measures include temporarily restricting access to any information or Tealium Systems in order to mitigate risks associated with further compromise, Tealium will promptly notify Customer of the restricted access in advance of such restriction when reasonably possible. Tealium will cooperate with Customer to identify any additional steps required of Tealium to address the Security Incident and mitigate its effects.

3.2.4. Unsuccessful Security Incident. Any Unsuccessful Security Incident will not be subject to this Section.

4. Independent Risk Assessments and Audits. Tealium has processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to support the secure Processing of Customer Data. These include the following:

4.1. Compliance Reports and Third-Party Audits. Tealium will undertake at least annually, at its expense, an audit in accordance with ISO/IEC 27001, and with the System and Organization Controls (SOC) Report under the SSAE-18 ("SOC 2") or their successor standard(s), covering controls related to the Tealium System. Additional Tealium certifications and attestations can be found in the Trust Center.

4.2. Sub-processor Agreements. Tealium will conduct a detailed risk assessment on its Sub-processors who process Customer Data with results documented and made available to Customer upon written request.

4.3. Security Testing. Penetration Testing of Tealium Systems related to the provision of Services will be performed quarterly. The method of test scoring and issue ratings will follow Industry Standard practices, such as the latest Common Vulnerability Scoring System ("CVSS") published by the US National Institute of Standards and Technology ("NIST"). Tealium's internal security operations team will evaluate all PenTests findings and Tealium will remedy any validated findings following completion of the evaluation as follows:

Emergency (< 7days)	CVE rating of 9.0 - 10.0 and/or remotely exploitable and rated **Emergency** by Tealium and exploit code is verified in the wild.
Critical (< 14 days)	CVE rating of 9.0 - 10.0 and/or remotely exploitable and rated **Critical** by Tealium
High (< 30 days)	CVE rating of 7.0 - 8.9 and/or remotely exploitable and rated **High** by Tealium
Medium (< 90 days)	CVE rating of 4.0 - 6.9 and rated **Medium** by Tealium
Low (< 180 days)	CVE rating of 0.0 - 3.9 and rated **Low** by Tealium

4.4. Sub-Processor Audits. Each of Tealium's Sub-processors maintains an information security program for the relevant services that complies with either SOC2 or the ISO/IEC 27001 standards or other alternative standards that are substantially equivalent to SOC 2 or ISO/IEC 27001 for the establishment, implementation, control, and improvement of the security standards applicable to such Sub-processor. Each Sub-processor uses external auditors to verify the adequacy of its security measures, including where applicable, the security of the physical data centers from which Tealium provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to SOC 2 or ISO/IEC 27001 standards or other alternative standards that are substantially equivalent to SOC 2 or ISO/IEC 27001; and (c) will be performed by independent third-party security professionals. Upon Customer's written request, Tealium will provide Customer with a report of Tealium's due diligence of Tealium's Sub-processors (the "**Sub-processor Report**"). Customer acknowledges that the Sub-processor Reports shall be considered Tealium Confidential Information as well as confidential information of the applicable Sub-processor. Any audit of Tealium Systems as described below will not include the physical data centers that are part of the Tealium Systems. Notwithstanding anything to the contrary in this DSS or the MSA, audits of the data centers are satisfied by the terms set forth in this Section 4.4.

4.5. Customer Audits (No Penetration Testing). Customer agrees that, to the extent applicable, Tealium's then-current SOC2 audit report (or comparable industry standard successor reports) and/or Tealium's ISO certifications will be used to satisfy any audit or inspection requests by or on behalf of Customer, and Tealium will make such reports or certifications available to Customer via the Trust Center.

In addition, Customer may conduct, either itself or through a third-party independent contractor selected by Customer at Customer's expense, an audit of the Tealium Systems used to provide the Services (each a "**Tealium Audit**"). A Tealium Audit shall be conducted no more frequently than one time per year, with 30

days' advance written notice unless required by applicable laws and regulations or following a Security Incident affecting Customer Data.

Any audits described in this Section shall be conducted during reasonable times, be of reasonable duration, not unreasonably interfere with Tealium's day-to-day operations, and be conducted in accordance with appropriate technical and confidentiality restrictions. Before any Tealium Audit commences, Customer and Tealium shall mutually agree upon the start date, the scope, timing, and duration of the Tealium Audit, any security and confidentiality controls applicable to the Tealium Audit. Customer shall pay Tealium for the costs of the resources expended by or on behalf of Tealium to support the Tealium Audit using Tealium's then-standard rate for such services.

In the event that Customer conducts an audit through a third-party independent contractor, prior to the audit beginning, such third party auditor shall be required to enter into a non-disclosure agreement with Tealium containing confidentiality provisions substantially similar to those set forth in the MSA to protect Tealium's Confidential Information. Customer is responsible for the costs of any third party auditor. Tealium may object in writing to such third party auditor, if in Tealium's reasonable opinion, the auditor is not suitably qualified or is a direct competitor of Tealium. Any such objection by Tealium will require Customer to either appoint another auditor or conduct the audit itself. Any expenses incurred by an auditor in connection with any review of audit reports or certifications or an audit shall be borne exclusively by Customer

4.6. Customer Audits (With Penetration Testing). Subject to the procedure set forth in Section 4.5 above for all Tealium Audits, in case an audit includes Penetration Testing, such test shall be coordinated with Tealium's security operations team and performed in a non-production environment running software with identical functionality to the production environment and in accordance with Tealium's vulnerability disclosure policy viewable at https://tealium.com/vdp. Any PenTests shall not exceed two (2) calendar weeks unless agreed upon by both parties. PenTests will be supported during Tealium's normal business hours (Monday through Friday 8 am to 5 pm PST). PenTest environments shall only be scaled to the function of the test and not to a production scale. Any information arising from a PenTest is Tealium's Confidential Information.

4.7. Findings and Remediation. Customer must promptly provide Tealium with all information and reports in an unredacted format regarding any vulnerabilities or gaps discovered during the course of an audit. Any information arising from a Tealium Audit or PenTest is Tealium's Confidential Information. Tealium agrees to discuss any such vulnerabilities or gaps with Customer upon Customer's request.

In the event that Tealium agrees to remedial actions or mitigations in response to a Customer Audit or PenTest, Tealium will provide a mitigation plan with supporting timelines. For Penetration Tests these timelines will align with Tealium's Vulnerability and Patch Management timelines.

5. Security Function.

5.1. Security Officer. Tealium will designate a point of contact to coordinate the continued security of all Customer Data and Tealium Systems**.** The Tealium Security Officer can be contacted at compliance@tealium.com.

5.2. Training. Tealium will, at least annually, provide all Tealium personnel with responsibilities related to the Services with appropriate ongoing information security and privacy training. All personnel involved in any part of Tealium's SDLC are required to receive secure code training. Tealium will retain documentation that such training has been completed.

6. Data Management. The following will apply to the Tealium Systems that Process Customer Data:

6.1. Data Access. Customer Data will be accessible only by Tealium personnel whose responsibilities

require such access and follow the principle of Least Privilege. Tealium will use Industry Standard authentication and authorization practices and secure all communications involving Customer Data access.

6.2. Encryption of Information. Tealium will use Industry Standard Encryption techniques for Customer Data being stored, processed, or transmitted by Tealium in the course of providing Services. Such techniques will require at least (a) key length of 256 bits or more for symmetric Encryption and (b) key length of 2048 bits or more for asymmetric Encryption. Tealium shall encrypt Customer Data at rest and in transit between untrusted networks (e.g. the Internet).

6.3. Cryptographic Key Management. Tealium will securely manage cryptographic keys using secure key management systems and maintain documented Industry Standard control requirements and procedures for encryption key management.

6.4. Removable Media. Tealium does not use Removable Media in providing the Services.

6.5. Data Disposal and Servicing. In the event that any hardware, storage media, or documents containing Customer Data must be disposed of or transported for servicing, then:

6.5.1. Tealium will maintain documented policies and procedures concerning data retention and disposal that include provisions to maintain chain of custody; and

6.5.2. Tealium will render such Customer Data inaccessible, cleaned, or scrubbed from such hardware and/or media using methods at least as protective as the minimum sanitization recommendations outlined by NIST SP 800-88 Rev.1 (or successor standard).

6.6. Data Transmission. When Customer Data is transferred by Tealium across the Internet, or other public or shared network, Tealium will protect such data using appropriate cryptography as required by Sections 6.2 and 6.3 of this DSS.

6.7. Data Resiliency. Tealium will utilize Industry Standard safeguards to provide resiliency of Customer Data. Resiliency will be achieved by use of services or methods such as, but not limited to, database backups, file backups, server backups, use of multiple availability zones within a single Region, or managed highly available services, fault tolerant data storage, or managed database services. Any Tealium storage or retention of backup files will be subject to all terms of this DSS. Tealium will test data resiliency periodically to protect the integrity and availability of Customer Data.

7. Physical and Environmental Security. Tealium ensures that appropriate physical and environmental controls are implemented at all data centers. Data centers used by Tealium will be protected by perimeter security such as barrier access controls (e.g., the use of entry badges) that provide a physical environment secure from unauthorized access, damage, and interference.

8. Tealium Systems Security.

8.1. Asset Inventory. Tealium will maintain a comprehensive inventory of current Tealium Systems (components, hardware, and software including version numbers and physical locations) to ensure only authorized and supported components comprise the Tealium Systems. Tealium will, at least annually, review and update its system component inventory.

8.2. Tealium Network Security. All data entering the Tealium network from any external source (including, without limitation, the Internet), must pass through Firewalls to enforce secure connections between internal Tealium network and external sources. Such Firewalls will explicitly deny all connections other than the minimum required to support Tealium business operations.

8.3. Intrusion Detection System. Intrusion Detection Systems will run on individual hosts or devices on Tealium Systems to monitor the inbound and outbound connections and will alert administrators if suspicious activity is detected. IDS will monitor file integrity of Tealium Systems and, if critical system files are modified, the IDS will log the event in Tealium's security information and event management systems. Tealium's Intrusion Detection Systems will monitor and log privileged command execution and be implemented in such a way as to identify Malicious Code (e.g. root kits, backdoors, reverse shells) on hosts.

8.4. Protect Against Malicious Code. Tealium will implement appropriate technical measures designed to protect against transferring Malicious Code to Customer systems via email or other electronic transmission. Security tools are deployed in Tealium Systems providing or supporting Services to Customer, and such tools are updated to provide protection against current threats.

8.5. Vulnerability Management. Tealium has a documented process to identify and remediate security vulnerabilities affecting Tealium Systems containing Customer Data.

8.6. Electronic Communications. All electronic communications related to the provision of Services, including instant messaging and email services, will be protected by Industry Standard safeguards and technical controls.

9. Change and Patch Management.

9.1. Change Management. Changes to applications, any part of Tealium's information technology infrastructure, and/or the Tealium Systems will be tested, reviewed, and applied using a documented change management process and adhere to the principle of Separation of Duties.

9.2. Emergency Changes. Tealium uses an emergency change approval process to implement changes and fixes to the Tealium Systems and Services on an accelerated basis when necessary. Tealium will notify Customer in advance if any such emergency changes could affect the functionality of Services.

9.3. Patch and Software Updates Management. Tealium will:

9.3.1. maintain a patch and vulnerability management process;

9.3.2. use security software in support of the delivery of Services;

9.3.3. use only supported versions of software required for the delivery of Services; and

9.3.4. where Services may be impacted, implement emergency software fixes within a reasonable time, unless, in Tealium's reasonable opinion, this introduces higher business risks. All changes are undertaken in accordance with Tealium's approved change management process.

10. Logical Access Controls.

10.1. User Authentication: Tealium will implement processes designed to authenticate the identity of all users through the following means**:**

10.1.1. User ID. Access to applications containing Customer Data must be traceable to one user. Shared accounts accessing Customer Data are prohibited by Tealium.

10.1.2. Passwords. Each Tealium user on Tealium Systems will use a unique password or equivalent secret to access applications containing Customer Data. Passwords will be at least eight (8) alphanumeric characters. The use of passwords that are easily discerned will be avoided (i.e., passwords matching or containing User ID, users' birthdays, street addresses, children's names, etc.). Tealium will require users

to use Multifactor Authentication for access to applications or systems containing Customer Data**.**

10.1.3. Single Sign On and Multifactor Authentication. Single sign on and Multifactor Authentication will be required for entry to all Tealium Systems to restrict entry to only authorized personnel.

10.2. Session Configuration. Sessions with access to Customer Data will be configured to timeout after a maximum of 60 minutes of user inactivity. Re-authentication will be required after such timeouts or periods of inactivity.

10.3. Unsuccessful Logon Attempts. The number of unsuccessful logon attempts will be limited to a maximum of five (5). User accounts will be locked for at least ten (10) minutes after the maximum number of permitted unsuccessful logon attempts is exceeded.

10.4. Remote Access. Remote access to Tealium Systems containing Customer Data will be restricted to authorized users, will require Multifactor Authentication, and will be logged for review.

10.5. Deactivation. User IDs for Tealium personnel with access to Customer Data will be deactivated immediately upon changes in job responsibilities that render such access unnecessary or upon termination of employment.

10.6. Privileged Access. Tealium will use Industry Standard methods to provide that:

10.6.1. Tealium users with access to Tealium Systems containing Customer Data will be granted the minimum amount of privileges necessary to perform their jobs;

10.6.2. privileged access will be restricted to authorized individual users and non-repudiation will be maintained;

10.6.3. privileged user accounts will be used exclusively for privileged operational use and not for business as usual activities;

10.6.4. developers may receive limited privileged access to production environments solely in managed circumstances where such access is necessary for the operation and support of the Tealium Systems; and

10.6.5. all privileged access will require Multifactor Authentication.

11. Logging & Monitoring.

11.1. Tealium Network Monitoring. Tealium will actively monitor the Tealium network supporting the Services where Customer Data is Processed to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.

11.2. Event Logging. For the Tealium Systems Processing Customer Data Tealium will:

11.2.1. maintain logs of key security events, including access events, that may reasonably affect the confidentiality, integrity, and/or availability of the Services to Customer and that may assist in the identification or investigation of Security Incidents occurring on Tealium Systems. Copies of applicable logs will be made available to Customer upon written request;

11.2.2. protect logs against modification or deletion;

11.2.3. review the logs on a regular basis;

11.2.4. store logs in an Industry Standard format; and

11.2.5. retain logs for at least twelve (12) months.

12. Software Security Assurance.

12.1. Development Methodology. For software used in the course of providing Services, Tealium will:

12.1.1. carry out in-house development activities in accordance with a documented secure SDLC, which will be shared with Customer upon written request;

12.1.2. deploy new applications and changes to existing applications to the live production environment strictly in accordance with the SDLC; and

12.1.3. maintain documented SDLC practices including requirements analysis, systems analysis, requirements definition, systems design, development, integration and testing, change acceptance, deployment, and maintenance.

12.2. Development Environments. For software used in the course of providing the Services, Tealium will perform system development and testing in distinct environments segregated from the production environment and protected against unauthorized disclosure of Customer Data.

12.3. Capacity and Performance Planning. Tealium will use capacity and performance planning practices and/or processes designed to minimize the likelihood and impact of Tealium Systems failures or outages. Tealium will review capacity plans and performance monitoring information on a regular basis.

12.4. Software Security Testing Process. Tealium will in the course of providing Services:

12.4.1. provide that applications undergo a formal code review process;

12.4.2. upon Customer's written request, Tealium will provide evidence of this formal code review process to Customer.

12.4.3. provide that applications undergo Dynamic Application Security Test (DAST), Software Composition Analysis (SCA) and Static Application Security Test (SAST), where the method of test scoring and issue ratings will follow Industry Standard practice, such as the latest Common Vulnerability Scoring System (CVSS) published by NIST; and

12.4.4. provide that applications undergo a Threat Model analysis. Tealium has a process to formally report the results of the Threat Model and to remediate material findings. Upon Customer's written request, Tealium will evidence this activity by sharing the Threat Model executive summary.

13. Data Center Controls.

13.1. Base Requirements. Any data center supporting the Services will possess the following minimum requirements:

13.1.1. Adequate physical security and access controls as set forth in Sections 6 and 7 of this DSS;

13.1.2. Industry Standard HVAC & environmental controls;

13.1.3. Industry Standard network/cabling environment;

13.1.4. Industry Standard redundant and high capacity networking bandwidth;

13.1.5. Industry Standard fire detection/suppression capability;

13.1.6. Industry Standard uninterruptible power distribution; and

13.1.7. A comprehensive business continuity plan.

14. Business Continuity Plan (BCP).

14.1. BCP Planning and Testing

14.1.1. Tealium's plan capabilities will include data resiliency processes covering all hardware, software, communications equipment, and current copies of data and files necessary to perform Tealium's obligations under the MSA; and

14.1.2. Tealium will maintain processes for timely recovery of Services.

14.2. BCP Plan. The plan will address the following additional standards or equivalent in all material respects:

14.2.1. regulatory requirements and Industry Standards;

14.2.2. include a business impact analysis of the expected impacts that Tealium believes are likely to arise in the event of a disruption to or loss of Tealium's normal operations, systems and processes;

14.2.3. the establishment and maintenance of alternate sites and systems, the capacity of which will be no less than the primary sites and systems that Tealium uses to provide the Services and perform its other obligations under the MSA;

14.2.4. a description of the recovery process to be implemented following the occurrence of a disaster. The description will detail the contingency arrangements in place to ensure recovery of Tealium's operations, systems and processes and the key personnel, resources, services and actions necessary to ensure that business continuity is maintained; and

14.2.5. a schedule of the objective times by which Tealium's operations, systems and processes will be recovered following the occurrence of a disaster. Tealium agrees that its recovery processes and BCP plans provide a Recovery Time Objective (RTO) of four (4) hours and a Recovery Point Objective (RPO) of 24 hours.

14.3. Notification. In case of a disaster that Tealium reasonably believes will impact its ability to perform its obligations or affect the Services under the MSA, Tealium will promptly notify Customer of such disaster. Such notification will, as soon as such details are known, describe:

14.3.1. The disaster in question and how it was detected;

14.3.2. The impact the disaster is likely to have on the Services;

14.3.3. The alternative operating strategies and the back-up systems Tealium will utilize and the timetable for their utilization; and

14.3.4. The expected timeframe in which the disaster will be resolved and Tealium expects to return to business as usual.

14.4. Sub-processors. Tealium will require its Sub-processors that perform any part of the Services (other than auxiliary services that facilitate the Services (e.g., document warehousing and retrieval, print services, etc.)) to have in place and maintain a commercially reasonable business continuity program that complies with regulatory and industry best practices. Tealium's use of Sub-processors does not diminish its obligation to provide business continuity capabilities as described above for all Services provided under the MSA, regardless of their origin and regardless of notice to Customer.

TEALIUM INC. DATA PROCESSING ADDENDUM
(Addendum DPA)

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"). This DPA supersedes all prior agreements on the subject matter whether signed or incorporated by reference (for example via a URL link).

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:

"APPI" means the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020).

"Customer Data" shall have the meaning set forth in the MSA.

"Data Exporter" and **"Data Importer"** have the meanings given to them in the Standard Contractual Clauses (as defined herein).

"Data Protection Laws and Regulations" means all laws and regulations that relate to the confidentiality, integrity, processing and/or protection of Personal Data including those 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, the APPI, PIPEDA, and the US Privacy Laws.

"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.

"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.

"Prohibited 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 2.

"**PIPEDA**" means the Canadian Personal Information Protection and Electronic Documents Act.

"Privacy Act" means the Australian Privacy Act 1988 (Cth.).

"Processing" or **"Process"** means any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as viewing, 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.

"**Sell**" and "**Share**" shall have the meaning set forth in the CCPA.

"Service Provider" shall have the meaning set forth in the CCPA.

"Standard Contractual Clauses" means the Annex to the European Commission Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 and, where applicable, the UK Addendum.

"Security Incident" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, but does not include any Unsuccessful Security Incident.

"Tealium Systems" means the data center, servers, networking equipment, applications, 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.

"UK Addendum" means the UK Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under S119A (1) Data Protection Act 2018.

"UK GDPR" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

"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.

"US Privacy Laws" means all US State laws that govern the Processing of Personal Data including the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq (the ("**CCPA**"), as amended by the California Privacy Rights Act of 2020 ("**CPRA**") as codified at Cal. Civ. Code Part 4, Division 3, Title 1.81.5 Section 1798.100 et. seq. as amended or supplemented from time to time and all similar US state privacy law or regulation.

"User Data" shall have the meaning set forth in the MSA.

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.

2.2 Compliance with Laws. Tealium will comply with all Data Protection Laws and Regulations applicable to it and binding on it in the provision of Services under the MSA, including all statutory requirements relating to data protection. Where applicable, Tealium will comply with the additional obligations required by Data Protection Laws and Regulations set forth in Appendix 1 of this DPA.

2.3 Instructions for Data Processing.

2.3.1 Tealium will Process Personal Data on behalf of and only in accordance with Customer's documented instructions, which include, without limitation, Customer's configuration of the Services, instructions contained in a Service Order or SOW, and/or instructions contained in this DPA and the MSA, and 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 the applicable legal requirement before Processing, unless such law prohibits such information on important grounds of public interest. Tealium certifies that it will not Sell or Share Personal Data.

2.3.2 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 is 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 obligations and shall comply with them. Processing outside the scope of this Section 2.3 (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.

2.3.3 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 until Customer has confirmed or changed such instruction.

2.4 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. Tealium will refrain from disclosing Personal Data to the respective authorities until a competent court of last instance has issued a final order for disclosure. Upon request, Tealium will provide Customer with general information on requests received from public authorities regarding Personal Data Processed under the MSA (at least number of requests, type of requested data, requesting body, and number of requests with confidentiality obligations).

2.5 User Data. As part of the Services, Tealium collects and uses User Data: (a) to allow authorized users to access and use the Services and communicate with Tealium regarding the Services; and (b) to develop, improve, support, and operate Tealium's products and services.

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. Security Responsibilities of Tealium. Tealium will:

4.1 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, 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 9 of this DPA for engaging a sub-processor;

4.3 taking into account the nature of the processing, assist Customer via 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 taking 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 required by applicable law, and cooperation with supervisory authorities.

4.5 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 Systems and associated Services to determine whether additional or mitigating security measures are required to respond to new security risks or findings identified by the periodic reviews. Tealium conducts ongoing vulnerability scans and annual penetration tests to identify and then remediate identified deficiencies. The Tealium Systems 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.

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.

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 written request, provide assistance to Customer in responding to such Data Subject Request.

6. Transfers of Personal Data.

6.1 Regions. Customer may specify the location(s) where Personal Data will be hosted at rest within the Tealium System. The list of hosting locations can be found at Tealium Sub-Processors Page as updated by Tealium from time to time (each a "Region"). Once Customer has made its choice during deployment of the Services, Tealium will not transfer the at-rest 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 is hosted in the USA.

6.2 Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to Personal Data that is transferred outside the EEA, Switzerland or the UK (as applicable), either directly or via onward transfer, to any country not recognized by the European Commission, the Federal Council or the UK Secretary of State (as applicable) as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses will not apply if Tealium has adopted an alternative recognized compliance standard for the lawful transfer of personal data outside the EEA, Switzerland or the UK in accordance with Article 46 of the GDPR/UK GDPR.

6.3 Where applicable under Section 6.2: (i) the Standard Contractual Clauses will be applied as described in Appendix 3 to this DPA; and (ii) the Standard Contractual Clauses will prevail to the extent of any conflict with the terms of this DPA.

6.4 Data Privacy Framework. Tealium has certified to the EU-U.S. Data Privacy Framework ("DPF") and adheres to the DPF Principles. Tealium's certification can be found here.

7. Certifications and Audits.

7.1 Tealium Audits. Tealium audits its security measures at least annually. These audits will be performed according to ISO 27001 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.

7.2 Audit Reports. Customer may access a copy of Tealium's audit reports and certifications at trust.tealium.com to verify Tealium's compliance with its obligations under this DPA. The report constitutes Tealium's Confidential Information.

7.3 Customer Audits. Customer's audit rights are as set forth in the DSS.

8. Security Incident Notification.

8.1 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.

8.2 The notification referred to in Section 8.1 shall at least:

8.2.1 describe the nature of the Security Incident;

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

8.2.3 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.

8.3 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.

8.4 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.

8.5 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 8.1 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.

8.6 Unsuccessful Security Incidents. Customer agrees that an Unsuccessful Security Incident will not be subject to this Section 8.

8.7 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.

8.8 Liability. Tealium's obligation to report or respond to a Security Incident under this Section 8 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. Sub-Processing.

9.1 Authorized Sub-processors. Customer agrees that Tealium may use the sub-processors set forth at Tealium Sub-Processors Page to fulfill certain of its contractual obligations under this DPA or to provide certain services on Tealium's behalf. Tealium will inform Customer at least 30 days in advance of any intended changes concerning the addition or replacement of sub-processors, thereby giving Customer the opportunity to object to such changes. Notice may include an update to the Sub-Processors Page and providing Customer with a mechanism to obtain notice of that update.

9.2 Obligations in respect of sub-processors. Where Tealium authorizes any sub-processor as described in this Section 9:

9.2.1 Tealium will restrict the sub-processor's access to Personal Data to only 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;

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

9.2.3 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.

9.3 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 20 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, unused fees for the period following the effective date of termination in respect of such terminated Services.

10. 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.

11. Termination of the DPA. This DPA shall continue in force until the later of the termination of the MSA or the period thereafter during which Tealium continues to be in possession of the Personal Data.

12. Return and Deletion of Customer Personal Data. The Services provide Customer with controls that Customer may use to retrieve or delete Personal Data at any time. Up to the termination date of the MSA, Customer will continue to have the ability to retrieve or delete any retained Personal Data in accordance with this Section. To the extent Customer is unable to retrieve or delete such Personal Data itself through its use of the Services, Tealium will assist Customer in such retrieval or deletion upon Customer's written request. Provided Customer has given notice of termination or expiration of the MSA, Tealium will delete retained Personal Data within 90 days following the termination date of this MSA. In any event, Tealium will delete retained Personal Data within 180 days following the termination date.

13. Fees and Expenses. 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, unless such change is required to fulfill Customer's obligations under applicable law.

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

15. 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.

Appendix 1 of the DPA – Specific Jurisdiction Provisions

Australia

The following provisions apply to all transfers from Customer to Tealium of Personal Data, the Processing of which is subject to the Privacy Act 1988 ("**the Act**") and the Australia Privacy Principles ("**APPs**") contained in the Act now in force or that may in the future come into force governing the protection of personal information of individual or individuals ("**Australia Personal Data**"):

(a) Tealium shall Process the Australia Personal Data in accordance with this DPA.

(b) Customer shall provide adequate notice and obtain appropriate consents as required by the Act/APPs.

(c) Tealium shall implement security measures designed to protect Australia Personal Data consistent with the Data Security Statement.

(d) Both Parties shall comply with all valid requests made by competent legal authorities.

(e) Upon request by Customer, Tealium shall provide Customer with the opportunity to retrieve the Australia Personal Data, consistent with Section 12 of the DPA.

Canada

The following provisions apply to all transfers from Customer to Tealium of Personal Data, the Processing of which is subject to the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") as amended or supplemented from time to time, and any similar Canadian federal or provincial legislation now in force or that may in the future come into force governing the protection of personal information of individuals ("**Canada Personal Data**"), where Customer acts as a Controller of the Canada Personal Data, and Tealium acts as a Processor of the Canada Personal Data:

(a) Tealium shall Process the Canada Personal Data in accordance with this DPA.

(b) Customer shall provide adequate notice and obtain appropriate consents as required by PIPEDA.

(c) Tealium shall implement security measures designed to protect Canada Personal Data consistent with the Data Security Statement.

(d) Both Parties shall comply with all valid requests made by competent legal authorities.

(e) Upon request by Customer, Tealium shall provide Customer with the opportunity to retrieve the Canada Personal Data, consistent with Section 12 of the DPA.

Japan

The following provisions apply to all transfers from Customer to Tealium of Personal Data, the Processing of which is subject to the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020) ("**APPI**") as amended or supplemented from time to time, and any similar Japanese federal or provincial legislation now in force or that may in the future come into force governing the protection of personal information of individuals ("**Japan Personal Data**"), where Customer and acts as a Personal Information Controller ("**PIC**") of the Japan Personal Data, and Tealium process Personal Data under the instructions of the PIC:

(a) Tealium shall Process the Japan Personal Data in accordance with this DPA.

(b) Customer shall provide adequate notice and obtain appropriate consents as required by the APPI.

(c) Tealium shall implement security measures designed to protect Japan Personal Data consistent with the Data Security Statement.

(d) Both Parties shall comply with all valid requests made by competent legal authorities.

(e) Upon request by Customer, Tealium shall provide Customer with the opportunity to retrieve the Japan Personal Data, consistent with Section 12 of the DPA.

California, United States

The following provisions apply to all transfers from Customer to Tealium of Personal Data and processing of Personal Data by Tealium that is subject to the CCPA ("**California Personal Data**"), where Customer acts as a Business with respect to Personal Data and Tealium acts as a Service Provider of California Personal Data:

(a) Tealium acknowledges that Customer is disclosing California Personal Data in connection with the MSA only for the limited and specified purposes of receiving the Services.

(b) Tealium shall retain, use, disclose, or otherwise Process California Personal Data solely on behalf of Customer for the specific purpose of providing the Services or as otherwise required by law. Tealium's Processing of California Personal Data shall, at all times, be done in compliance with the MSA, and this DPA.

(c) Tealium shall not:

i. retain, use, disclose, or otherwise Process California Personal Data except as necessary to provide the Services or as otherwise required by law.

ii. Sell California Personal Data.

iii. Share California Personal Data.

iv. Process California Personal Data in any manner outside of the direct business relationship between the Parties.

v. Combine any California Personal Data with Personal Information that it receives from or on behalf of any other third party, provided that Tealium may combine California Personal Data for a Business Purpose if directed to do so by Customer or as otherwise expressly permitted by the CCPA.

(d) Tealium agrees to cooperate with any reasonable and appropriate audits in accordance with the audit provisions of the Data Security Statement. Tealium agrees to immediately notify Customer in writing if it can no longer comply with the CCPA or its obligations under the MSA or this DPA. Any subcontracting of Services will be as set forth in the DPA. Tealium agrees to cooperate with Customer in responding and implementing verifiable Consumer requests to exercise rights afforded to Consumers by the CCPA, including by assisting with appropriate technical and organizational measures as further described in the DPA. Deletion of California Personal Data shall be as set forth in the DPA.

Appendix 2 to the DPA - Scope of Processing

For purposes of this Appendix 2, Customer is the data exporter and Tealium is the data importer.

Categories of data subjects whose personal data is transferred
Data exporter may submit personal data to the 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) visitors to data exporter's websites, mobile applications or other digital or physical properties; (b) other persons whose personal data is uploaded to the Services by the data exporter; (c) data exporter's employees or agents who are users of the Services.

Categories of personal data transferred
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. Data exporter acknowledges that data importer does not monitor and will be generally unaware of the types of data processed within the Services.

Sensitive data transferred
Data exporter determines and controls the scope of personal data Processed subject to limitations in the MSA, including those relating to Prohibited Data.

The frequency of the transfer
Continuous

Nature of the processing
The data importer hosts the platform where data processing is carried out in accordance with data exporter's instructions and configuration of the Services.

Purpose(s) of the data transfer and further processing
The purpose of the Processing of personal data by data importer is the performance of the Services pursuant to the MSA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
For the duration of the MSA or as specified by the data exporter from time to time through its configuration of the Services via the user interface.

Appendix 3
Application of the Standard Contractual Clauses

1. Clause 7 shall/shall not be applicable.

2. With respect to clause 9(a), Option 2 (General written authorisation) will apply. The time period is to be 30 days.

3. With respect to clause 11, the Option shall/shall not be applicable.

4. With respect to clause 17, Option 1 shall apply.
The Member State is:
If not specified, the Member State where the data subject is located.

5. With respect to clause 18(b) the Member State is:
If not specified, the Member State where the data subject is located.

6. With respect to Annex I to the Clauses:

A. LIST OF PARTIES

The data exporter is: The entity identified as “Customer” in the DPA and the MSA
Activities relevant to the data transferred under these Clauses: Access to and use of web services
Role (controller/processor): Controller or processor

The data importer is: Tealium Inc., 9605 Scranton Road, Suite 600, San Diego, CA 92121, USA
Activities relevant to the data transferred under these Clauses: Provision of web services
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

As set forth in Appendix 2.

C. COMPETENT SUPERVISORY AUTHORITY:

If not specified, the Competent Supervisory Authority is the one located where the data subject is located.

7. With respect to Annex II to the Clauses, the description of the technical and organisational measures implemented by the data importer is as set forth in the Data Security Statement.

8. Where the provision of Services involves the transfer of Personal Data from Switzerland, the Parties agree to the Standard Contractual Clauses as incorporated into this DPA with the following modifications:
(a) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss

Federal Data Protection Act (“FDPA”) and references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section the FDPA;

(b) references to "EU", "Union" and "Member State" shall be replaced with references to the Switzerland;

(c) the "competent supervisory authority" shall be the Swiss Federal Data Protection and Information Commissioner;

(d) in Clause 17, the EU SCCs shall be governed by the laws of Switzerland; and

(e) in Clause 18(b), disputes shall be resolved before the courts of Switzerland.