Tealium Privacy Statement
Effective as of January 1, 2020

1 Purpose and Scope

1.1 Purpose

This Privacy Statement will help you understand what Personal Data we collect about you, how we use your Personal Data, and what choices you have about our use of your Personal Data. This Privacy Statement applies to your use of any online service (website, software or mobile app) that include a link to this Privacy Statement, regardless of how you use or access it. When we refer to “Tealium” “we” or ‘us” in this Privacy Statement, we are referring to Tealium Inc.

We are committed to maintaining the accuracy, confidentiality, and security of your Personal Data. Tealium utilizes data centers around the world in order to facilitate our customers’ ability to store Personal Data regionally.

We comply with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (“Privacy Shield”) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data transferred from the European Union, the United Kingdom, and Switzerland to the United States in reliance on Privacy Shield. We have certified to the Department of Commerce that we adhere to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. With respect to Personal Data received or transferred pursuant to the Privacy Shield, Tealium is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

We are committed to complying with the Privacy Shield Principles with respect to your Personal Data that we receive from the EU, the United Kingdom, and Switzerland in reliance on the Privacy Shield. One of the purposes of this Privacy Statement is to describe how Tealium implements the Privacy Shield Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability in processing your Personal Data.

This Privacy Statement includes a description of the purposes for which we collect and use Personal Data, the types of Personal Data we collect, the types of third parties to which we may disclose your Personal Data and the purposes for doing so, the rights and choices you have for limiting the use and disclosure of your Personal Data, and how to contact us about our practices concerning Personal Data.

To learn more about the EU and Swiss Privacy Shield, visit the U.S. Department of Commerce’s Privacy Shield site. To view Tealium’s certification see the list of participating companies and search for "Tealium".

Inquiries or Concerns? In compliance with the Privacy Shield Principles, we are committed to resolving complaints about our collection or use of your Personal Data. EU, UK, and/or Swiss individuals with inquiries or complaints regarding our Privacy Statement should first contact us
at: privacy@tealium.com. We have also appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this Privacy Statement. If you have any questions about this Privacy Statement, including any requests to exercise your legal rights, you may contact our DPO at dpo@tealium.com.

We will endeavor to answer your questions and advise you of any steps taken to address the issues raised by you. We have further committed to refer unresolved Privacy Shield complaints through the Privacy Shield Arbitration Process and the JAMS Privacy Shield Program, an alternative dispute resolution provider with offices in the United States and Europe. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact or visit the JAMS Privacy Shield Program for more information or to file a complaint. The services of JAMS are provided at no cost to you.

If you are unsatisfied with our response, you may be entitled to make a written submission to the EU, UK, or Swiss data protection authorities established pursuant to the Privacy Shield to address your complaints applicable for your jurisdiction. Under certain conditions, more fully described on the Privacy Shield website, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

1.2 Scope
This Privacy Statement applies to the Personal Data of individuals who seek to be, are, or were customers of Tealium (“Customers”), including any Personal Data of individuals collected, used, or disclosed while using the Tealium websites or Tealium apps (“Site Visitors”). It is important that the Personal Data we hold about you is accurate and current. Please keep us informed if your Personal Data changes during your relationship with us.

Revisions to this Privacy Statement. We may revise this Privacy Statement to reflect changes in our legal or regulatory obligations or in the manner in which we deal with your Personal Data. We will communicate any revised version of this Privacy Statement and such revisions will be effective from the time they are communicated, provided that any change that relates to why we collect, use or disclose your Personal Data will not apply to you, where your consent is required to such collection, use or disclosure, until we have obtained your consent to such change.

Our websites and our services are not intended for children and we do not knowingly collected data from or relating to children. If you are a parent or guardian and you believe that your child has provided us Personal Data without your consent, please contact us at privacy@tealium.com and we will delete the child’s Personal Data from our systems.

2 Policy

2.1 Notice

2.1.1 What is Personal Data?

For the purposes of this Privacy Statement, Personal Data is information, including Sensitive Data, that is: (i) about an identified or identifiable individual, (ii) received by us, and (iii) recorded in any form. Personal Data does not include anonymous or non-personal information (i.e.,
information that cannot be associated with or tracked back to a specific individual). “Sensitive Data” means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

2.1.2 What Personal Data Do We Collect?

We may collect and maintain Personal Data regarding Site Visitors and Customers and potentially their customers. We may collect, use, store and transfer different kinds of Personal Data about you which we have grouped together into the following categories:

- Data used to identify you, including first name, last name, username or similar identifier, title, and gender.
- Contact information such as email address and telephone numbers.
- Technical information such as internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- Profile information such as your interests, preferences, and feedback.
- Usage information about how you use our website, products, and services.
- Marketing and communications information such as your preferences in receiving marketing from us and your communication preferences.
- If you attend one of our events, we may ask you to scan your attendee badge, which will provide to us your Personal Data, such as name, title, company name, address, country, phone number and email address.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data may be derived from your personal data, but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your usage data with the data of other Site Visitors to calculate the percentage of users accessing a specific website feature.

2.1.3 For What Purposes Do We Collect Personal Data?

The Personal Data we collect is used and disclosed, as reasonably required for our business purposes, including complying with our contractual requirements, legal obligations, and for legitimate interests in marketing and product functionality purposes. Broadly speaking, legitimate interest means we use the personal information you provide to us for our legitimate business interests to send you marketing communications or to gather information about how you use our website. Before doing this, though, we will also carefully consider and balance any potential impact on you and your rights. How we collect your Personal Data and how we use it are described below:

- We use cookies to make your interactions with the Tealium website easy and helpful. When you visit our website, our servers send a cookie to your device. Cookies that are used as part of the services (in the proxy) may include cookies of a third party website that is being co-browsed,
for example, in order to deliver the website as intended by the third party website operator. Our services may also use tracking pixels embedded by our Customers in their online advertising, often distributed to third party websites using ad exchanges, that allow Customers to gather data about viewers of their online advertising. For more information on how Tealium uses cookies, please see here.

- We may use web beacons alone or in conjunction with cookies to compile information about Customers’ and Site Visitors’ use of the Tealium website and interaction with emails from Tealium. For example, we may use web beacons to count the number of Site Visitors and to count content views. Web beacons are transparent pixel images that are used in collecting information about website usage, e-mail response, and tracking.

- We collect information about our Site Visitors’ utilization and navigation of our website as legitimate interest in prospective customers. This information helps us to design our website to better suit our Site Visitors’ needs. We may also use your IP address to help diagnose problems with our server and to administer our website, analyze trends, track Site Visitor movements, and gather broad demographic information that assists us in identifying Site Visitor preferences.

- We use aggregated data as a statistical measure and not in a manner that would identify you personally. Aggregated data enables us to determine how often certain parts of our website or the Services are used so that we can improve them. We may make use of, or make such aggregated data available to, third parties, in any manner in our sole discretion. Tealium may engage third parties to track and analyze usage and volume statistical information from Site Visitors.

- Our website may allow you to connect with social media networks, such as Facebook (facebook.com), Linkedin (linkedin.com), and Twitter (twitter.com) (“Social Media”). Such Social Media may collect your IP address and which page you are visiting on our website, and may set a cookie to enable the Social Media to function properly. You may be given the option by such Social Media to post information about your activities on our website to your profile page on the Social Media network in order to share with others within your network.

- We may contract with third-party advertising networks (“Ad networks”) that collect IP addresses and other information from our website, from emails, and on third-party websites. Ad networks follow your online activities over time by collecting information through automated means, including through the use of cookies. They use this information to provide advertisements about products and services tailored to your interests. You may see these advertisements on other websites. This process also helps us manage and track the effectiveness of our marketing efforts. We may also partner with third parties to provide certain features on our websites or to display advertising based upon your web browsing activity. You have the ability to opt out of advertising through our Consent Manager.

- Our services provide Customers a platform that may collect data, including Personal Data, from their customers and to use that information to create real-time profiles of such customers that integrate with their digital marketing platforms. We do not control our Customers’ use of the Personal Data, and their use of the information will be in accordance with their own privacy policies.
Our platform may analyze the information collected from a website, ours or our Customers’, in order to create segments of customers and to combine these segments into audiences in order to enrich the capabilities of the website and to correlate data across various customer-consumer touch points such that our Customers gain a unified view of their customers profiles. We do not control our Customers’ use or collection of the Personal Data, and their use of the information will be in accordance with their own privacy policies.

2.1.4 What Types of Third Parties May Receive Your Personal Data and for What Purposes?

Service Providers
- We may share Personal Data with Tealium’s contracted service providers, such as payment processors, so that these service providers can provide services on our behalf. We may also share Personal Data with our service providers to ensure the quality of information provided. Unless described in this Privacy Statement, we do not share, sell, rent, or trade any information with third parties for their promotional purposes.

Tealium Affiliates
- We may share Personal Data with other members and affiliates of the Tealium corporate group in order to work with them, including affiliates of the Tealium corporate group. For example, Tealium may need to share Customer Information for customer relationship management purposes.

Partners and Affiliated Businesses Not Controlled by Tealium
- We may partner with other companies to jointly offer products or services. If you purchase or specifically express interest in a jointly offered product or service from us, we may share Personal Data collected in connection with your purchase or expression of interest with our partners. We do not control our partners’ use of the Personal Data, and their use of the information will be in accordance with their own privacy policies. If you do not wish for your information to be shared in this manner, you may choose not to purchase or specifically express interest in a jointly offered product or service.

Billing
- We may use a third-party service provider to manage credit card processing. This service provider is not permitted to store, retain, or use financial information except for the sole purpose of credit card processing on our behalf.

Compelled Disclosure
- It may be necessary for us to disclose your Personal Data, either by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate. We may also disclose Personal Information about you if we
determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users.

Relevant information also may be found in notices pertaining to specific data processing activities.

2.2 Choice
We offer Site Visitors and Customers who provide contact information the means to choose how we use the information provided. You may manage your receipt of marketing and non-transactional communications by clicking here or by clicking on the “unsubscribe” link located on the bottom of Tealium’s marketing emails. Additionally, you may send a request specifying your communications preferences to privacy@tealium.com. Customers cannot opt out of receiving transactional emails related to their account with Tealium or the Services.

To update financial information or have your registration information deleted, please email support@tealium.com. To discontinue your account, please email support@tealium.com. Requests to access, change, or delete your information will be handled within 30 days.

Individuals have a right to choose whether their Personal Data may be disclosed to third-party controllers or used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the individual. We do not typically collect Sensitive Data about you. If we were to collect Sensitive Data, to the extent required by the Privacy Shield Principles, Tealium will obtain your opt-in consent for certain uses and disclosures of Sensitive Data. You have a right to withdraw such consent at any time. If we decide to use Personal Data for a purpose other than those that are materially the same as those indicated in this Privacy Statement, individuals shall be offered the opportunity to opt-in to the use. We shall make reasonable efforts to accommodate individual privacy preferences.

Exceptions. We may disclose your Personal Data without offering an opportunity to opt out, when (i) we retain third-party processors to perform services on our behalf and pursuant to our instructions, (ii) required by law or legal process, or (iii) responding to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. We may also transfer Personal Data in the event of an audit or if we sell or transfer all or a portion of our business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution, or liquidation).

2.3 Accountability for Onward Transfer
We comply with the Privacy Principles for all onward transfers of Personal Information from the UK, the EU, and Switzerland, including the onward transfer liability provisions.

2.4 Security
We take reasonable and appropriate measures that are designed to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration, and destruction, taking into account the nature of the Personal Data. Tealium has a SOC2 Type 2 audit, an ISO 27001
audit, and ISO 27018 audit performed regularly to independently assess and attest to the effectiveness of Tealium’s information security policies and practices.

2.5 Data Integrity and Purpose Limitation
We limit the Personal Data we process to that which is relevant for the purposes of the particular processing. We do not process your Personal Data in ways that are inconsistent with the purposes for which the information was collected or subsequently authorized by you. In addition, to the extent necessary for these purposes, we take reasonable steps to ensure that the Personal Data we process is (i) reliable for its intended use, and (ii) accurate, complete and current. In this regard, we rely on you to update and correct Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized by you. You may contact us as indicated in the Subject Access procedure in section 2.10 below to request that we update or correct relevant Personal Data. If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Subject to applicable law, we retain Personal Data in a form that identifies or renders you identifiable only for as long as it serves a purpose that is compatible with the purposes for which the Personal Data was collected or subsequently authorized by you.

2.6 Access
You have the right to access your Personal Data. Accordingly, where appropriate, we provide you with reasonable access to the Personal Data we maintain about you. We also provide you a reasonable opportunity to choose whether to receive offers and promotions from us and correct, amend, or delete your information.

We may limit or deny access to Personal Data where the burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated. Other reasons for denying or limiting access include (i) interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial; (ii) disclosure where the legitimate rights or important interests of others would be violated; (iii) breaching a legal or other professional privilege or obligation; (iv) prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or (v) prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.

Please contact privacy@tealium.com as described in section 2.10 to request access to your Personal Data.

2.7 Recourse, Enforcement, and Liability
We have mechanisms in place designed to help assure compliance with the Privacy Shield Principles. We conduct an annual self-assessment of our Personal Data practices to verify that the attestations and assertions we make about our Privacy Shield privacy practices are true and
that our privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.

You may file a complaint concerning Tealium’s processing of your Personal Data. We will take steps to remedy issues arising out of our alleged failure to comply with the Privacy Shield Principles. You may contact us as specified in the Grievance procedure in section 2.11 below about complaints regarding our Personal Data practices.

If your complaint regarding Personal Data cannot be resolved through our internal processes, we will cooperate with the Swiss Federal Data Protection and Information Commissioner (FDPIC), the Information Commissioner’s Office in the UK, or a panel of EU data protection authorities established pursuant to the Privacy Shield to address your complaints and provide you with appropriate recourse free of charge. We are also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

2.8  Opt-in

If we decide to process Personal Data for purposes other than those contained in this Privacy Statement, affected Customers and Site Visitors will receive a notice detailing:

a. the type of Personal Data to be processed;
b. the purpose for the processing and a description of how the processing is based on legitimate interests;
c. the categories of recipients of disclosures of the Personal Data;
d. the period for which the Personal Data will be stored or the criteria for determining the period;
e. how Customers and Site Visitors can exercise the rights of access, correction, erasure, objection, and the right to withdraw consent;
f. the right to file a complaint with the Swiss Federal Data Protection and Information Commissioner (FDPIC), the Information Commissioner’s Office in the UK or a Data Protection Authority;
g. whether the Customer or Site Visitor is obliged to provide the data by statute, contract, or for another reason, and the possible consequences of failing to provide the data; and
h. whether the Personal Data will be subject to automated processing and, if so, the logic and the consequences of the processing for the data subject.

Such notices will be clear, conspicuous, and readily available to affected Customers and Site Visitors. A notice will require an unambiguous, affirmative, opt-in consent to the particular use or processing of the Customer’s or Site Visitor’s Personal Data.

2.9  Third-Party Controller Transfers

With respect to transfers of your Personal Data to third-party data processors, we will:

a. enter into a contract with each relevant data processor,
b. transfer Personal Data to each such data processor only for limited and specified purposes, including prohibiting such data processor from selling, renting or using your Personal Data in any way outside of our instructed use,

c. ascertain that the data processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the Privacy Shield Principles,

d. take reasonable and appropriate steps to ensure that the data processor effectively processes the Personal Data in a manner consistent with Tealium’s obligations under the Privacy Shield Principles,

e. require the data processor to notify Tealium if the data processor determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles,

f. upon notice, including under (e) above, take reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the data processor, and

g. provide a summary or representative copy of the relevant privacy provisions of the data processor’s contract to the US Department of Commerce, upon request.

Tealium remains liable under the Privacy Shield Principles if the company’s third-party data processor onward transfer recipients process the relevant Personal Data in a manner inconsistent with the Privacy Shield Principles, unless Tealium proves that it is not responsible for the event giving rise to the damage.

2.10 Subject Access Rights and other rights that you have to your Personal Data

You have rights under data protection laws in relation to your Personal Data. These rights include the following:

• To request access - this allows you to receive a copy of the Personal Data we hold about you.

• To request correction – this allows you to have any incomplete or inaccurate Personal Data corrected or amended.

• To request deletion or erasure – this allows you to have your Personal Data deleted where there is no reason for us to continue to process it. You may also ask us to delete or remove your Personal Data where you have successfully exercised your right to object to processing if we processed your information unlawfully or if we are required to erase your personal data to comply with local law. We may not always be able to comply with your erasure request if specific legal reasons apply. In such case, we will let you know if these reasons apply at the time of your request.

• To object to processing – this allows you to object to use of your Personal Data where we are relying on a legitimate interest (or those of a third party) but you believe that such use impacts your fundamental rights and freedoms. You may also object where we are processing your personal data for direct marketing purposes. In some cases, we may
demonstrate that we have compelling legitimate grounds to process your Personal Data which override your rights and freedoms.

• To request transfer – this allows you to request that we transfer your Personal Data to you or to a third party of your choice.

• To withdraw consent – this allows you to withdraw your consent to our processing of Personal Data where we are relying on your consent to process the data.

• To exercise any of the rights stated above, please email us at privacy@tealium.com.

2.11 Grievance procedure
You may file a complaint concerning Tealium’s processing of Personal Data by email at privacy@tealium.com. If a failure to comply with the Privacy Shield Principles is found, we will take steps to remedy the issue.

If a complaint regarding Personal Data cannot be resolved through our internal processes, we will cooperate with the Swiss Federal Data Protection and Information Commissioner (FDPIC), the Information Commissioner’s Office in the UK or a panel of EU Data Protection Authorities established pursuant to the Privacy Shield to address a complaint and provide appropriate recourse free of charge. We are also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

2.12 Data Breach
If a breach of Personal Data occurs, we will notify the relevant Data Protection Authorities within 72 hours, subject to likelihood of risk to the Customer or Site Visitor. Affected Customers or Site Visitors will also be notified regarding the breach.

2.13 Auditing compliance
To verify that this Privacy Statement has been implemented as represented, we will conduct an annual audit and self-assessment of our Personal Data security and privacy practices.

2.14 Record-keeping
We will maintain relevant records of:

a. the purposes of Personal Data processing;

b. the categories of data subjects and of Personal Data processed;

c. the categories of recipients, including those in third countries;

d. the third countries to which Personal Data will be transferred and the instrument used to provide an adequate level of protection;

e. where possible, the envisaged retention periods for different categories of Personal Data; and

f. a general description of the security measures used to protect Personal Data.
These records shall be provided to the Swiss Federal Data Protection and Information Commissioner (FDPIC), the Information Commissioner's Office in the UK or the EU Data Protection Authorities upon request.

2.15 Customer Notice

Swiss, UK, and EU Customers will be given a notice concerning the processing of their Personal Data during the onboarding process. This notice will explain how their Personal Data will be processed during the customer relationship, including:

- the purposes for the processing and when the processing is based on legitimate interests, a description of those interests;
- the categories of recipients of disclosures of Personal Data;
- that the controller intends to transfer Personal Data to a third country and the legal basis for the transfer;
- the period for which the Personal Data will be stored or the criteria for determining the period;
- how Customers can exercise the rights of access, correction, erasure, and objection;
- where processing is based on consent, the right to withdraw consent;
- the right to file a complaint with the Swiss Federal Data Protection and Information Commissioner (FDPIC), the Information Commissioner's Office in the UK, or the EU Data Protection Authorities;
- whether the Customer is obliged to provide the data by statute, contract, or for another reason, and the possible consequences of failing to provide the data; and
- whether the Personal Data will be subject to automated processing and, if so, the logic and the consequences of the processing for the data subject.

Your California Privacy Rights

Tealium honors Do Not Track (DNT) headers and allows its users to opt-out of having their personal information collected by Tealium. We also provide guidelines and instructions on how to honor DNT headers. The behavior of utag.js can be altered to track only analytic data and not track individual visitors. Tealium’s website honors DNT and is compliant with California Assembly Bill 370.

This section provides additional details about the personal information we collect about California consumers and the rights afforded to them under the California Consumer Privacy Act (“CCPA”).

Starting January 1, 2020, California consumers will have more control over the personal information that covered businesses collect about them. Among other things, consumers will have the right to obtain a copy of the personal information collected about them in the last 12 months, the right to request to know more details about the categories or specific pieces of
personal information we collect (including how we use and disclose this information), opt out of
the sale of their personal information and/or request the deletion of their personal information,
and to not be discriminated against for exercising these rights.

California consumers may exercise these rights by clicking here or they may contact us at
privacy@tealium.com to exercise any of your rights under the CCPA. We will verify our request
using the information associated with your account. We may also ask you for additional
identification information.