

Tealium の顧客保護のパッケージ (「CPP」) に関する FAQ

当 FAQ をご覧いただきありがとうございます。当 FAQ は、Tealium がすべてのお客様に提示しお約束する顧客保護および努力を記載する文書を含む顧客保護パッケージに関する便利な情報を提供するためにデザインされました。CPP は、Tealium がすべてのお客様に提供する保護とその達成のための努力を記載する文書です。当 FAQ は情報提供のみを目的とし、当事者が考慮の対象とする契約の一部を成すものではありません。DSS および DPA のすべての責任に関する問題は、MSA に記載があります。

CPP の構成

CPP は 3 つの文書からなっています。:

サービス水準契約書(「SLA」) は、すべての本サービスを通して Tealium のサポートが利用可能であることを約束するための Tealium の努力、極めて稀ではありますがその努力が達成されなかった場合のお客様の救済が含まれます。

データセキュリティー規定 (「DSS」) には、顧客データを保護するため Tealium が形式化した組織的および技術的セキュリティー保護対策が含まれます。

データ処理契約書 (「DPA」) は、適用されるプライバシー保護法および規律に則った Tealium のデータ処理の取り組みの詳細が含まれます。

SLA

Tealium には、リアルタイムのステータスおよびメンテナンスや緊急停止をお知らせするウェブサイトがあります。<https://status.tealium.com> からご覧いただけます。Tealium は、稀ではありますが、SLA にある取り組みを実行できなかった場合の救済、また長期に及ぶ停止状態になった場合の契約解除の権利を提供します。SLA がすべての商品を通じて提供されていること、またマルチテナントの SaaS サービスを提供していることから、個々のお客様に合わせて SLA を変更することはできません。我々は SLA が業界水準に達しており、お客様のすべての問題に対応できると確信しています。

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 commitment 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.

<p>DSS</p> <p>データセキュリティ規定を使う必要がある理由 - 何が含まれるのか？</p> <p>本 DSS は、お客様の本サービスの購入に関する契約書の一部、およびお客様によって、またはお客様のために本サービスに送信されるすべての電子データと情報（本サービスの使用から派生する拡張と出力を含む）（「顧客データ」という）についての内容を構成します。DSS は、すべてのお客様に同等に適用される、顧客データのための Tealium のセキュリティの方針および対策を反映します。</p> <p>Tealium がいかにして本サービスに送信される個人データを保護するか。</p> <p>Tealium が個人データ保護のために整備しているデータ機密性保護のプログラムおよび対策の詳細は、データ処理補填(「DPA」)に定義されています。</p> <p>自分のデータセキュリティ文書ではなく Tealium の DSS を使う理由</p> <p>以下の特別な理由により、お客様に提供されるデータ保護に関する文書ではなく、我々の DSS を使用しなければなりません。</p> <p>本サービスは「皆のための一つの」モデルを使ってお客様に提供されます。つまり、同じ本サービスがすべてのお客様に提供されることとなります。ですので、あるお客様（またはそのデータ）に対し、別のお客様とは異なる方法でのサービス提供を可能にする「カスタマイズ」されたサービスは提供しておりません。</p> <p>特別な目的（サポートのリクエストなど）のためにお客様から指示がない限り、または MSA に基づいて別途許可される場合を除き、我々がおお客様の顧客データにアクセスすることはありません。我々がおお客様の顧客データにアクセスするようお客様に指示された場合は、お客様がアクセスの範囲を設定し、またいつでも我々のアクセスを終了することができます。そのため、Tealium は顧客データに関する以下の項目に関して管理しません。：</p> <ul style="list-style-type: none"> • データの性質（データの匿名性、個人情報または秘密情報か否かを含むがこれに限らない）、 	<p>DSS</p> <p>Why do we need a Data Security Statement and what does it cover?</p> <p>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 customer equally.</p> <p>How does Tealium protect personal data submitted to the Services?</p> <p>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”).</p> <p>Why do we need to use the Tealium DSS instead of our own data security documentation?</p> <p>There are specific reasons why we offer a DSS instead of using the data security addendums provided by our customers.</p> <p>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.</p> <p>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 in the MSA. If you instruct us to access your Customer Data, you control the access permissions and can terminate our access at any time.</p> <p>As such, we do not control any of the following with respect to your Customer Data:</p> <ul style="list-style-type: none"> • 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;
--	--

- アカウント内の顧客データを保存または構成する特定の手法、
- データが誰に関連するか、
- データ処理の目的、
- データ送信先である第三者、および
- あるデータおよび/または処理方法がデータ対象者にリスクを課すか否か（またはその程度）。

我々の本サービスは業界に依存しない性質を持つため、我々は、あるデータのどの部分が国および・または業界特有の規制に制限を受けるかを判断することはできません。

Tealium の厳格なセキュリティー制御は、すべてのお客様に同等に利益をもたらします。同じ本サービスがすべてのお客様に提供されているため、皆様に共有された技術的および組織的なセキュリティー保護をどなたでも受けることができます。

法的要件に関する DSS の記載

お客様の顧客データに関する法的要件が満たされているかどうかを確認するためにはお客様が重要な役割を果たします。例えば、我々が、包括的な技術的かつ組織的対策（多くの監査の実行やサティフィケーションの提供を含む）を行なっていることはご存知の通りですが、本サービスがお客様の特定の使用に適しているか、また本サービスがお客様の特定の顧客データに対するセキュリティーおよび法的条件を満たすかどうかを判断するためには、最終的にお客様が不可欠な役割を果たすこととなります。

顧客は簡単に Tealium の TOMS 追加情報にアクセスできる？

はい。Tealium のセキュリティー措置は、trust.tealium.com（「トラストセンター」）にて詳細が記載されています

DPA

データ処理補填を使う必要がある理由 - 何が含まれるのか？

本データ処理補填（「DPA」）は、お客様による本サービスの購入に関する契約書の一部を構成

- 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.

し、顧客データに含まれるすべての「個人データ」（DPAに定義される）をカバーします。Tealiumは、お客様が本サービスに送信する個人データのデータ処理者またはサービス提供者として機能します。我々のDPAは、本サービス内で処理される個人データのためのプライバシー保護プログラムを反映し、該当するデータ保護法に基づくTealiumの義務に対応します。

Tealiumのお客様には、世界的に事業を運営される方がいるため、我々のDPAは、随時修正または変更される、欧州連合規制 2016/679（「GDPR」）、米国プライバシー法（DPAに定義）、カナダ個人情報保護および電子文書法（「PIPEDA」）、1988年オーストラリア連邦プライバシー法（Cth.）、および個人情報保護法（2020年改定の2003年版法番号57）の追加条件を含む、世界のデータ保護の要件に対応します。

自分のデータ処理文書ではなく Tealium の DPA を使う理由

以下の特別な理由により、お客様のデータ処理文書ではなく Tealium の DPA を使用しなければなりません。

1. 本サービスは「皆のための一つの」モデルを使ってお客様に提供されます。つまり、同じ本サービスがすべてのお客様に提供されることとなります。ですので、あるお客様（またはそのデータ）に対し、別のお客様とは異なる方法でのサービス提供を可能にする「カスタマイズ」されたサービスは提供しておりません。実装やサポートなどの補助的サービスもまた、同等の方法ですべてのお客様に提供されます。カスタマイズされたサービスは提供できませんが、お客様のデータ処理要件に従って本サービスを設定することができ、またお客様のアカウントの特定の地理的ホストロケーションをお選びいただけます（DPAに詳細を定義）。

2. 我々の本サービスのすべては業界に依存しない性質を持つため、我々は、個人データのどの部分が業界特有の規制に制限を受けるかを判断することができません。

Tealiumの統一された厳格なセキュリティー制御は、すべてのお客様に同等に利益をもたらします。同じ本サービスがすべての

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

お客様に提供されているため、皆様に共有された技術的および組織的なセキュリティ保護をどなたでも受けることができます。

3. 我々の HIPAA クラウドサービスは、米国 HIPAA 規定に準拠するため、強化されたセキュリティ保護対策を含みます。PHI を Tealium に送信し、HIPAA クラウドサービスを購入される場合、Tealium からビジネス提携契約書をお求めください。

Tealium の個人データを保護するためにデザインされた技術的および組織的なセキュリティ対策の整備

Tealium は、不法なまたは偶発的損害、紛失、変更、無許可の開示、またはアクセスに対して、個人データを保護するためにデザインされた、強固な技術的および組織的対策を整備しています。

Tealium のセキュリティ対策は trust.tealium.com (「トラストセンター」) に詳細が記載され、データセキュリティ規定または DSS で定義されています。

DPA は GDPR28 条(3)の条件を含む GDPR に対応している？

我々の DPA は、GDPR28 条(3)の条件を含む GDPR の条件に対応するため特別に作成されました。GDPR の条件が満たされているかの判断において、お客様は重要な役割を担っています。例えば、我々は、包括的な技術的かつ組織的対策（多くの監査の実行やサティフィケーションの提供を含む）について透明性を維持していますが、本サービスがお客様の特定の使用に適しているか、また本サービスがお客様の特定の個人データに対する条件を満たすかどうかは、最終的にお客様が判断する必要があります。

DPA は CCPA (CPRA による変更を含む) などの米国プライバシー法に対応している？

DPA は、CPRA によって変更され更新される CCPA の条件に対応します。DPA セクション 2 は、Tealium がお客様の個人データを売却または共有しないことを記載しています。Tealium は、お客様の指示なしに、または MSA に基づいて別途許可される場合を除き、お客様の個人データを使用

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, Tealium has implemented robust technical and organizational measures designed to protect against unlawful or accidental destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Tealium's security measures are detailed at trust.tealium.com ("Trust Center") and summarized in the data security statement or DSS.

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

せず送信しません。前述の通り、どのように CCPA の条件のいくつかが満たされているかの判断において、お客様は重要な役割を担っています。例えば、我々は、包括的な技術的かつ組織的対策（多くの監査の実行やサティフィケーションの提供を含む）について公表していますが、本サービスがお客様の特定の使用に適しているか、また本サービスがお客様の特定の個人データに対する条件を満たすかどうかは、最終的にお客様が判断する必要があります。

国境を超えたデータ送信について

個人データがある地域から別の地域に送信される中、Tealium は、お客様が Tealium のサービスの使用に関連して実行されるデータ影響評価に必要なすべての情報を提供します。Tealium が提供する支援と保護措置のより詳しい内容は <https://tealium.com/data-transfer/> およびトラストセンターにて閲覧可能です。

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.

サービス水準契約書 (SLA)

本サービス水準契約書(「SLA」)は、基本サービス契約書(MSA)、本サービス条件、または本 SLA 補足規定を参照する本サービス注文書に組み込まれまたその一部となり、Tealium と顧客間の MSA の一部を構成する（かかる本サービス注文書に示される通り）。

1. 定義。 次に定義された語句は本 SLA 補足規定にて使用される。:

「**利用可能な**」または「**利用可能性**」とは、本サービスが機能する状態であり、また（API、タグ、HTTP リクエスト/応答などの）プログラム、または特定の本サービスに適用可能なユーザーインターフェースを通じて本サービスへのアクセスが可能な状態をさす。本配信ネットワークのパフォーマンスにおいてのみ、「利用可能な」とは、本配信ネットワーク（以下定義）のサーバーがライブラリ（以下定義）へのリクエストに応答している状態をさす。

「**本配信ネットワーク**」とは、Tealium JavaScript ファイルまたはその他の本サービスに関連したファイル（以下「**ライブラリ**」という）を提供するための所定の本サービスに関連して使用されたコンテンツの配信ネットワーク・サービス・プロバイダをいう。

「**不可抗力**」とは、当事者が合理的に制御できない事由をいい、天候、公共施設もしくは通信サービス（インターネットへのアクセスを含む）が利用できないこと、市民による妨害、内乱、行政当局もしくは軍当局の行動、または天災を含むがこれに限らない。

「**月次加入額**」とは、本サービス期間の本サービスの契約金額を本サービス期間の月数で除算した金額（実装、管理および専門サービスの料金、また追加利用料金を除く）をいう。

「**月次使用可能時間率**」とは、ある暦月における本サービスが利用可能な時間の割合をいう。

「**本サービスクレジット**」とは、以下定義された条件で計算される、顧客に発行する未来の請求書に対して Tealium が充当することができるクレジットをいう。

2. 本サービス使用可能性の誓約。 Tealium は、いずれの月においても 99.9%以上の月次使用可能時間率で本サービスを利用可能にするように商業的

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

に合理的な努力を払うものとする（以下「本サービスの誓約」という）。本サービスが本サービスの誓約を満たさない場合には、顧客は、以下で定める本サービスクレジットを受け取る資格を有する。

3. 本サービスクレジット。本サービスクレジットは、本サービスの誓約が以下のスケジュールに従って満たされなかった月の、特定の本サービスにかかる月次加入額の割合として計算される。Tealium は、将来の支払のみに本サービスクレジットを充当するものとする。顧客が MSA に基づきすべての本サービスに対して全額を前払いする場合は、MSA が満了するか更新されなければ、顧客は Tealium へ書面上の要請をすることで本サービスクレジットの分の返金を受け取る権利を有する。本サービスが本サービスの誓約を満たすことができなかった場合、顧客の単独のかつ唯一の救済は本 SLA の条件に従って本サービスクレジットを受け取ることである。本サービスクレジットは、その他の顧客のアカウントに移転または充当することはできない。

本サービス水準(%)	クレジット (%)
98-99.89	5
95-97.99	10
<95	15

4. クレジットの要求および支払手続。本サービスクレジットを受け取るために、顧客は、services@tealium.com に電子メールメッセージを送信して、要求書を提出しなければならない。クレジット受給の資格を満たすには、クレジットの要求が、(a) Tealium のある月における本サービスの誓約を満たさなかったことも証明する、合理的に詳細な機能停止状況のリストを含み、(b) 電子メールの本文に、顧客が経験したとする各インシデントの日付および時間を記載し、(c) 顧客が主張する機能停止を文書化し、Tealium がかかる機能停止を立証できる顧客の追加情報（サーバーのリクエストログなど）（当該ログの秘密情報または機密情報は、削除するか、またはアスタリスクに置き換えなければならない）を含み、(d) サービスの誓約が満たされなかった月の末日から 10 営業日以内に Tealium が受領しなければならない。クレジットを受け取るには、当セクション 4

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 in which the Service

に従って Tealium が単独で、顧客の主張する機能停止を認めることができることが条件となる。

5. SLA の除外。 本サービスの誓約は、(a) Tealium が合理的に制御できない要素（不可抗力事由、または本配信ネットワークの責任分界点を超えるインターネットへのアクセスの問題もしくは関連する問題を含む）によって生じるか、

(b) 顧客もしくは第三者の作為もしくは不作為に起因するか、(c) 顧客の装置、ソフトウェアもしくは他の技術、および/もしくは第三者の装置、ソフトウェアもしくは他の技術（Tealium が直接管理する第三者の装置を除く）に起因するか、または (d) MSA に従って本配信ネットワークを使用する顧客の権利が停止し、終了したことから生じるか、(e) システムまたはネットワークのメンテナンスのために計画されたダウンタイムによる本サービスの利用停止または他の本配信ネットワークの性能の問題には適用されない。

6. 恒常的機能停止による契約解除の権利。 上記のセクション 3 に示される本サービスクレジットの救済に加え、2 ヶ月連続で、または 4 ヶ月分（連続した 12 ヶ月の間いつでも）、月次使用可能時間率が 95% を下回る場合は、顧客は意図された通り機能しない本サービス欠陥による本サービス注文書を解約し、有効な解約日の後、影響のあった期間に対し事前に支払われた金額分の返金を受け取ることができる。かかる解約が有効となるためには、かかる解約の通知を、解約する権利が生じた月から Tealium が 30 日以内に受領しなければならない。

7. Tealium 以外の商品; コネクター。 コネクターに不具合があったとする通知を、Tealium がコネクターからのエラーメッセージを受けるか、またはその通知を顧客から受けた場合、Tealium は 5 営業日以内にかかるコネクターの不具合について調査を行う。Tealium がコネクターを作成したところで、Tealium は商業的に道徳的な努力を払い、第三者のコネクターの提供元と協力してコネクターの不具合を修復し、また合理的に適切な時間内に第三者の提供元による解決策またはパッチを行うものとする。この条項に基づく一切の問題は利用可能性から特別に除外される。

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.
--	--

データセキュリティ規定(DSS)	DATA SECURITY STATEMENT (DSS)
<p>本データセキュリティ規定(「DSS」)は、Tealium と顧客間の MSA に組み込まれ、その一部となる。</p> <p>1. 一般。</p> <p>1.1 Tealium は、顧客データを処理する際、管理上、論理的かつ物理的なセキュリティ制御を実行し、また維持する。これらの制御は、顧客データの偶発的または違法な破壊、消失、変更、無許可の開示または無許可のアクセスに対する少なくとも業界基準(ただし、いかなる場合も本補足条項に定める特定の保護の強度を下回ってはならない)と同等の、合理的に適切な技術的および組織的保護措置を提供するようデザインされている。Tealium は、Tealium 本サービスの継続的機密性、整合性、可用性、および耐性を保証するための措置を講じる。Tealium は、業界基準の変化、新しいテクノロジーまたは新しい脅威の出現に応じて、定期的にそのセキュリティ基準および制御を再評価しまた変更する。両当事者による別段の合意がない限り、すべての顧客データ処理は、論理的に区分制御されたマルチテナント環境下で行う。</p> <p>1.2 顧客は、Tealium が、当 DSS に基づく Tealium の契約義務の一定の部分を満たし、または Tealium を代表して一定のサービスを提供するために、https://tealium.com/subprocessors/で定義されるサブプロセッサを使用することができることに合意する。Tealium は、DPA に示される通り、サブプロセッサの追加または代替に関するあらゆる意図的な変更について、顧客に少なくとも 30 日前にその旨を通知し、顧客がかかる変更に関する異議を唱える機会を与える。</p> <p>2. 定義。</p> <p>「ダイナミックアプリケーションセキュリティテスト」または「DAST」とは、あるアプリケーションを生産環境下で、または当該アプリケーションが稼動する生産環境を想定したテスト環境下で稼動させて、そのセキュリティの脆弱性を示す条件を探知するためにデザインされたアプリケーションのセキュリティテストをいう。</p> <p>「暗号化」とは、データの機密性を保護するため、暗号化されたアルゴリズムを用いてデータを</p>	<p>This Data Security Statement (“DSS”) is incorporated into, and made a part of, the MSA between Tealium and Customer.</p> <p>1. General.</p> <p>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.</p> <p>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.</p> <p>2. Definitions.</p> <p>“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.</p> <p>“Encryption” means the process of using a cryptographic algorithm to transform data from plain text to ciphertext in order to protect the confidentiality of the data.</p>

平文から暗号文に変換するプロセスをいう。

「ファイアウォール」とは、ネットワークコネクションのための既定のセキュリティールールを実行することによって、Tealium システムへの不正な電子アクセスを防止するために使用される統合的なセキュリティ措置の集合体をいう。

「業界基準」とは、MSA が対象とする種類のサービスの供給者たちが遵守している慣習および慣行であって、当該供給者たちに期待される技術、注意力、慎重さおよび洞察力を反映するものいう。

「侵入探知プロセス」または「IDP」とは、システムログおよびプロセスをほぼリアルタイムで、また、侵入の発生または侵入発生の可能性を示す動作パターンの増加をすみやかに、不合理に遅延することなく検知する方式をいう。

「最小限の権限」とは、特定のコンピュータ環境（例えば、個々の処理、ユーザーまたはプログラムなど）の下にあるどのモジュールも、適法正当な目的のために必要な情報およびリソースに限りアクセスが可能であることをいう。

「悪意のあるコード」とは、本サービス、すべての当事者のコンピュータまたは通信システム、ネットワーク、施設または機器を破壊し、損害を与え、あるいは妨害する目的で、またはかかるシステム、ネットワーク、施設または機器に無許可にアクセスする目的を持つコンピュータの指示またはソフトウェアコードをいう。害意コードの例は、ウイルスを含むあらゆるコード、トロイの木馬、ワーム、トラップ、スパイウェア、バックドア、機器の運転停止、もしくは同様の破壊的コードあるいは自動再生コードを含むがこれに限らない。

「多要素認証」とは、パスワードなどの「貴方が知っているもの」、トークンなどの「貴方が所有するもの」、または生体認証などの「貴方であるもの」のうち、少なくとも2つの要素を使う認証をいう。

「侵入テスト」または「PenTest」とは、手動および/または自動のアプリケーションのセキュリティテストをいい、自動ツール、有資格のテスター、および/または有資格の第三者の組み合わせによって実行される。

“**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,

「処理すること」または「処理」とは、顧客データに作動する、あらゆるオペレーションまたはオペレーションの集合体（自動装置によるものか否かに限らない）をいう。その例として、収集、記録、編成、構成、ストレージ、適合または変更、入手、参照、使用、送信による開示、流布またはその他の方法による公開、同調または結合、制限、消去または破棄などが挙げられる。

「リムーバブルメディア」とは、持ち運び可能なまたは取り外し可能な外部データ保存機器をいう。

「SDLC」とは、情報セキュリティー対策（特にデザイン、設計、テスト、および開発の工程時の対策）を必要とする情報システムの、プランニング、作成、テスト、およびデプロイに関する文書化されたプロセスである、セキュアソフトウェア開発ライフサイクル方式をいう。

「セキュリティーインシデント」とは、偶発的または違法な顧客データの破壊、損失、変更、無許可の開示あるいは顧客データへのアクセスに繋がる、無許可または違法なセキュリティーの侵害のすべてをいう。ただし未然のセキュリティーインシデントを除く。

「職務の分離」とは、一人の人間が重要な工程のセキュリティー管理方法を変えることができないよう、役割と責任を分割することをいう。

「ソフトウェア構成分析」または「SCA」とは、すべてのオープンソースソフトウェアおよび・または第三者のライブラリを含むあらゆる既存の脆弱性を、コードベース内で検知するセキュリティーテストをいう。

「静的アプリケーションセキュリティーテスト」または「SAST」とは、あるアプリケーションのコード内のセキュリティーの脆弱性を示す状態を検知するためにデザインされた、アプリケーションのソースコードのセキュリティーテストをいう。

「サブプロセッサ」とは、Tealiumと連携して、Tealiumを代表して顧客データの特定の処理活動を行うプロセッサをいう。

「Tealium システム」とは、Tealium またはその

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-

サブプロセッサの管理内にあり、かつ本サービスを提供するために使用される、データセンターサーバー、ネットワーク、ネットワーク環境、アプリケーションおよびホストソフトウェア（仮想ファイアーウォールなど）をいう。

「脅威モデル」とは、価値のある何かを保護する見地から潜在的な脅威および緩和を特定し、列挙し、優先順位をつけることをいう。

「トラストセンター」とは、trust.tealium.comで閲覧可能な Tealium の順守文書をいう。トラストセンターは、方針、自動監視データ、サブプロセッサなど、Tealium の順守文書を誰でも閲覧できる倉庫をいう。

「未然のセキュリティインシデント」とは、顧客データのセキュリティの危殆化に至らない未然の試みまたは活動をいう。これには、ファイアーウォールまたは端末サーバーへのピングおよびその他のブロードキャストの攻撃、ポートスキャン、未然のログインの試み、サービス攻撃の拒否、パケット盗聴（またはその他の、顧客データへのアクセスに至らないトラフィックへの無許可のアクセス）、もしくは同様のインシデントを含むがこれに限らない。

「根本原因分析」とは、セキュリティインシデントに関連する根本的原因を特定するための基本原理ベースのシステムアプローチをいう。

3. インシデント管理およびセキュリティインシデントの通知

3.1 インシデント管理。 Tealium は、セキュリティインシデントを適時に探知するため、文書化されたインシデント管理の方針および手順を整備し、脅威および顧客からの通知に対し連携した対応をとる。

3.2 セキュリティインシデントの通知と是正。 セキュリティインシデントが発生した場合、Tealium は顧客に通知し、以下に定める方法によりセキュリティインシデントを是正する。:

3.2.1 通知。 Tealium がセキュリティインシデントを確認した場合、不当な遅延なしに、可能な場合、確認した時点から 48 時間以内に顧客にセキュリティインシデントの通知をする。48 時

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

間以内に顧客が通知を受けなかった場合、当該遅延の理由が提供されなければならない。

通知には少なくとも以下の点が含まれなければならない。:

- (1) セキュリティーインシデントの性質の説明、
- (2) データ保護担当者またはより多くの情報が得られるその他の者の氏名と連絡先の詳細、および
- (3) Tealium がセキュリティーインシデントを是正するために講じた、または申し出た措置（悪影響が出る可能性がある場合、これを最低限に抑える適切な措置を含む）の説明。

情報の同時提供が不可能な場合、過度の遅延なく、段階ごとに情報が提供される。

Tealium は、あらゆるセキュリティーインシデント、セキュリティーインシデントに関する周辺事実、その影響および講じられた是正措置を文書化しなければならない。

3.1.2 根本原因分析。 Tealium は本原因分析をすみやかに開始し、不当な遅滞なく完了を目指す。

3.1.3 是正。 Tealium は、顧客データおよび Tealium システムの安全性を回復するために必要な措置を速やかに講じる。悪影響がさらに拡大するリスクを減じるため、当該措置により一切の情報または Tealium システムへのアクセスが一時的に制限される場合、Tealium は、当該制限に先立って、合理的に可能な時点で、アクセスの制限について顧客に速やかに通知をする。Tealium は、顧客と協力して、Tealium が漏洩に対処し、その影響を減じるために必要な追加的処置を特定する。

3.1.4 未然のセキュリティーインシデント。 未然のセキュリティーインシデントの一切は当セクションの対象とならない。

4. 独立のリスク査定および監査。 Tealium は、顧客データの安全な処理を補助するため、技術的かつ組織的措置の効率を定期的にテスト、査定および評価するシステムを持つ。そのシステムは以下を含む。:

4.1 順守に関する報告および第三者の監査

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 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.

。 Tealium は、少なくとも年に一度、自己の費用負担で、ISO/IEC 27001、および SSAE-18 に基づくシステムおよび組織の統制 (SOC) 報告書 (「SOC 2」)、またはこれらの後続の基準に従って、システムに関する制御について監査を実施する。追加の Tealium の認定および認証は、トラストセンターで閲覧可能である。

4.2 サブプロセッサの契約。 Tealium は、顧客データを処理する Tealium のサブプロセッサについて詳細なリスク査定を行う。その査定結果は文書化され、顧客は書面により要請すればこれを入手できる。

4.3 セキュリティーテスト。 本サービスの提供に関する Tealium システムの侵入テストは 3 ヶ月に一度行われる。テストの採点および問題評価の方法は、アメリカ国立標準技術研究所 (「NIST」) が公表する最新の共通脆弱性評価システム (「CVSS」) など、業界基準の慣行に従う。Tealium の内部セキュリティー管理チームはすべての侵入テスト結果を審査し、Tealium は、結果が確認された場合、以下の通り審査が完了した後、適時にこれを是正する。

緊急 (<7 日間)	CVE の値が 9.0 - 10.0、および・またはリモートで悪用可能かつ Tealium に 緊急 と評価され、悪用コードの被害が確認される。
重大 (<14 日間)	CVE の値が 9.0 - 10.0、および・またはリモートで悪用可能かつ Tealium に 重大 と評価される。
高 (<30 日間)	CVE の値が 7.0 - 8.9 、および・またはリモートで悪用可能かつ Tealium に 高 と評価される。
中 (<90 日間)	CVE の値が 4.0 - 6.9 、および Tealium に 中 と評価される。
低 (<180 日間)	CVE の値が 0.0 - 3.9 、および Tealium に 低 と評価される。

4.4 サブプロセッサの監査。 Tealium の各サブプロセッサは、当該サブプロセッサに適用されるセキュリティー基準の設立、実行、管理および改良において、SOC2 または ISO/IEC 27001 の基準、あるいは SOC2 または ISO/IEC 27001 と実質的

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-**

に同等のその他の代替基準のいずれかに準拠する、関連サービスの情報セキュリティプログラムを維持する。各サブプロセッサは、外部の監査法人を使って自身のセキュリティ対策の適性を検証する。そのセキュリティは、適用される場合、Tealium が本サービスを提供する物理的なデータセンターのセキュリティを含む。この監査は、(a)少なくとも年に一度、(b) SOC2 または ISO/IEC 27001 の基準あるいはその他の SOC2 または ISO/IEC 27001 と実質的に同等の代替基準に従って行われ、また(c)独立した第三者のセキュリティ専門家によって行われる。顧客の書面上の要請により、Tealium は顧客に、Tealium のサブプロセッサの精査報告書（「サブプロセッサ報告書」）を提供する。顧客は、サブプロセッサ報告書が Tealium の本秘密情報かつ該当するサブプロセッサの秘密情報と見なされなければならないことを認める。以下に示される Tealium のシステムの監査のすべては、Tealium のシステムの一部である物理データセンターを含まない。本 DSS または MSA 内のこれに反するすべてにかかわらず、データセンターの監査は、本セクション 4.4 に定義される条件を満たすことで十分であるとされる。

4.5 顧客の監査（侵入テストを除く）。 顧客は、該当する場合、Tealium のその時点での SOC2 監査報告書（または同等の業界基準の後継報告書）および、または Tealium の ISO 証明書が、顧客によるもしくは顧客を代表して要請されたあらゆる監査または点検の要件を満たすために使用されることに同意し、Tealium は、トラストセンターにてかかる報告書または証明書を提供する。

これに加えて顧客は、自身または顧客選定の第三者の独立した業者によって、顧客の自己負担で、本サービス提供のために使用される Tealium システムの監査を行うことができる（それぞれを「Tealium 監査」という）。Tealium の監査は、年に一度を超える頻度では行われず、書面による 30 日の事前通知を伴って行われなければならない（適用法に要求される場合、または顧客データに影響を与えるセキュリティインシデント後である場合を除く）。

当セクションに示される監査はすべて、適切な時間内に、Tealium の通常業務を非合理的に妨害せずに、また適切な技術的および秘密保護の制限に

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

基づいて行われなければならない。すべての Tealium の監査が始まる前に、顧客および Tealium は、開始日、監査内容、時間帯および Tealium の監査に要する時間、Tealium の監査に該当するセキュリティーおよび秘密情報の管理のすべてにおいて互いに同意しなければならない。顧客は、Tealium に、Tealium によってあるいは Tealium の代わりに支払われた、[Tealium](#) のその時に有効な当該サービスのための標準料金に則った [Tealium](#) の監査をサポートするための出費を支払う。

顧客が第三者の独立した業者に監査をさせる場合、かかる独立業者は、Tealium と、Tealium の本秘密情報を保護する MSA に定義される条項と実質的に同類の秘密保護の条項を含む秘密保護契約を、監査前に締結していなければならない。顧客はすべての第三者の監査人の費用を支払う責任がある。Tealium は、第三者の監査人に関して、Tealium の合理的な判断によって、かかる監査人が適任でない、あるいは Tealium の直接的な競合者であると認めた場合、書面によりかかる第三者の監査人選定に異議を唱えることができる。Tealium による異議を受けた場合、顧客は別の監査人を選任するか、自ら監査を行う必要がある。監査報告書または証明書の検討、あるいは監査に関連して監査人に発生するあらゆる費用は、顧客が単独で支払わなければならない。

4.6 顧客の監査 (侵入テスト)。 すべての Tealium の監査に関して、前述のセクション 4.5 に基づいて、ある監査が侵入テストを含む場合、当該テストは、Tealium のオペレーションチームと協力して、非生産環境で実行されるソフトウェアにおいて生産環境と同じ機能を用いて、また <https://tealium.com/vdp> にて閲覧可能な Tealium の脆弱性開示ポリシーに従って行われなければならない。すべての PenTest は、両当事者に別途合意がない限り、カレンダー上 2 週間を超えて行われてはならない。PenTest は、Tealium の通常営業時間（太平洋時間で月曜日から金曜日の午前 8 時から午後 5 時まで）の間サポートされる。PenTest の環境は、生産スケールではなく、テストの機能に見合ったスケールでのみ行われなければならない。PenTest で発生する情報のすべては Tealium の本秘密情報である。

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 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

4.7. 発見および救済措置。 顧客は、監査中発見されたすべての脆弱性またはセキュリティーギャップについて、Tealium に、すべての報告書を修正されていない状態で直ちに提出しなければならない。Tealium の監査または侵入テストから発生するあらゆる情報は、Tealium の本秘密情報である。
Tealium は、顧客の要請を受けた場合、当該脆弱性またはセキュリティーギャップのすべてについて議論することに同意する。

顧客の監査または侵入テストの結果を受けて Tealium が救済または緩和措置に同意した場合、Tealium は、サポートのタイムラインと共に緩和措置のプランを提供する。侵入テストの場合、これらのタイムラインは Tealium の脆弱性およびパッチ管理のタイムラインに合わせて作成される

5. セキュリティー機能。

5.1 セキュリティー担当者。 Tealium は、すべての顧客データおよび Tealium システムの継続的セキュリティー保護を図るため担当者を指定する。Tealium のセキュリティー担当者には、compliance@tealium.com で連絡をすることができる。

5.2 訓練。 Tealium は、少なくとも年に一度、本サービスに関係する責任を負うすべての Tealium の人員に対し、適切な継続的情報セキュリティーおよびプライバシー訓練を提供する。Tealium の SDLC 方式のいずれかの部分に関与するすべての人員は、安全コードの訓練を受けなければならない。Tealium は、かかるトレーニングが完了したことを示す記録を保管する。

6. データの管理。 顧客データを処理する Tealium システムには、以下が適用される。:

6.1 データへのアクセス。 顧客データには、職務上アクセスする必要があるかつ最小限の権限の原則に従う Tealium の人員のみがアクセスすることができる。Tealium は、業界基準の認証および認証慣行に従って顧客データに関わる全ての通信を保護する。

6.2 情報の暗号化。 Tealium は、本サービス提供において顧客データを保存し、処理または送信する場合には、業界基準の暗号化の技術を用いる。かかる技術は、少なくとも (i) 対称暗号化には

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

128 ビット以上のキーの長さ、および(ii)非対称暗号化には 2048 ビット以上のキーの長さを必要とする。Tealium は、信頼されていないネットワーク（インターネットなど）間で保存される、またはそこで通信される顧客データを暗号化しなければならない。

6.3 暗号化キーの管理。 Tealium は、安全なキー管理システムを用いて暗号化キーを安全に管理し、キー管理の暗号化のための文書化された業界基準の管理要件および手順を維持する。

6.4 リムーバブルメディア。 Tealium は、本サービスの提供にリムーバブルメディアを使用しない。

6.5 データの消去およびサービス。 顧客データを収納するハードウェア、保存メディア、または顧客データを含む文書を処分し、またはサービスのために移動する必要がある場合には、：

6.1.1 Tealium は、データの保存および処分に関する文書化された方針および手続（受け渡しの管理の維持に関する規定を含む）を遵守し、

6.1.2 Tealium は、当該ハードウェアおよび/またはメディアから、少なくとも NIST SP 800-88 Rev.1（または後続基準）が推奨する最低限のサニタイズの方法と同程度の保護の方法を用いて、当該顧客データをアクセス不能とし、除去し、または消去する。

6.6 データの通信。 顧客データが Tealium によってインターネット、またはその他の公共もしくは共同ネットワークを通じて送信される場合、Tealium は本 DSS セクション 6.2 および 6.3 の要求に従い適切な暗号を用いてデータを保護する。

6.7 データの復元力。 Tealium は、業界基準の保護機能を利用して顧客データを復元する。復元の方法としては、データベースのバックアップ、ファイルのバックアップ、サーバーのバックアップ、一つのリージョン内で利用できる複数のゾーンの利用、または管理された高可用性のサービス、耐障害性のデータ保存もしくは管理データベースサービスがあるが、これらに限定されない。Tealium のバックアップファイルの保管または保持は、すべて本 DSS の条件に従う。

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 use 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

7. 物理的および環境的セキュリティ。 Tealium は、適切な物理的および環境的管理がすべてのデータセンターで実行されることを保証する。

Tealium が使用するデータセンターは、出入口のアクセスの管理（例えば、入場証の使用など）のように不正のアクセス、毀損および妨害から防御された物理的環境を提供する周辺警備によって保護される。

8. Tealium システムセキュリティ。

8.1 資産目録。 Tealium は、現行の Tealium システム（バージョン番号および物理的所在地を含む、コンポーネント、ハードウェアおよびソフトウェア）の包括的な目録を維持し、権限のあるまたはサポートされたコンポーネントのみが Tealium システムを構成することを保証する。Tealium は、少なくとも年に一度、システムコンポーネントの目録を見直し、更新する。

8.2 Tealium のネットワークセキュリティ。 あらゆる外部ソース（インターネットを含むがこれに限らない）から Tealium のネットワークに入るすべてのデータは、Tealium の内部ネットワークと外部のソース間の安全な接続を確保するため、ファイアウォールを通過しなければならない。当該ファイアウォールは、Tealium の事業運営に必要な最小限のデータ以外のデータを明確に拒否する。

8.3 侵入検知システム。 侵入検知システムは、対内および対外コネクションを監視するため Tealium システム上の個々のホストまたは機器に対して実行され、不審なアクティビティが検知されると管理人に警告する。IDS は Tealium システムのファイルの生合成を監視し、重要なシステムファイルが変更された場合、IDS は Tealium のセキュリティ情報およびイベント管理システム内にかかるイベントを記録する。Tealium の侵入検知システムは、特権コマンドの実行を監視しまた記録し、ホスト上の悪意のあるコード（ルートキット、バックドア、リバースシェルなど）を検知するよう実行される。

8.4 悪意のあるコードからの保護。 Tealium は、

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.

悪意のあるコードの送信に対する保護を目的としてデザインされた適切な技術措置を、顧客のシステムに、email またはその他の電子送信によって実施する。セキュリティツールは、顧客にサービスを提供するすべての Tealium のシステムにデプロイされ、更新されて、現行の脅威に対する保護を提供する。

8.5 脆弱性の管理。 Tealium は、顧客データを収納する Tealium システムに影響を与える脆弱性を発見し、修復する文書化されたプロセスを備える。

8.6 電子コミュニケーション。 本サービスの提供に関連するすべての電子コミュニケーション（インスタントメッセージおよび Email サービスを含む）は、業界基準の処理方法および技術管理によって保護される。

9. 変更およびパッチ管理。

9.1 変更の管理。 アプリケーションの変更、Tealium の情報技術基盤のあらゆる部分の変更、Tealium システムの変更は、文書化された変更管理プロセスを用いてテスト、検査および実行され、職務の分離の原則に従う。

9.2 緊急変更。 Tealium は、必要に応じて迅速に、緊急変更の許可のプロセスを行い、Tealium システムの変更および修復を実行する。Tealium は、かかる緊急変更が本サービスの機能に影響を与える場合、顧客に事前に通知する。

9.3 パッチおよびソフトウェアのアップデートの管理。 Tealium は、：

9.3.1 パッチおよび脆弱性管理手順を維持し、

9.3.2 本サービスの提供のためのセキュリティソフトウェアを使用し、

9.3.3 本サービス提供に必要なサポートされるソフトウェアのバージョンのみを使用し、

9.3.4 本サービスが影響を受ける場合、より高い事業リスクがあると Tealium が合理的に判断しな

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 (1) user. Shared accounts accessing Customer Data are prohibited by Tealium.

10.1.2 Passwords. Each 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 designed 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

い限り、合理的な時間内にソフトウェアの緊急修復を行う。すべての変更は、Tealium が承認した変更管理プロセスに従って行われなければならない。

10. 論理的なアクセスコントロール。

10.1 ユーザー認証: Tealium は、以下の方法により、すべてのユーザーについて、本人確認のためにデザインされた手続を実行する。:

10.1.1 ユーザーID。 顧客データを収納するアプリケーションへのアクセスは、ユーザー1名に限定される。Tealium は、顧客データにアクセスできるアカウントの共用を禁止する。

10.1.2 パスワード。 Tealium システムの各ユーザーは、一意的なパスワードまたは同等に機密性を持つパスワードを使って顧客データを収納するアプリケーションにアクセスする。パスワードは、少なくとも 8 桁の英数字とする。容易に解析可能なパスワード (ユーザーID、ユーザーの誕生日、住所、子供の名前と同じまたはそれを含むパスワードなど) は拒否される。Tealium は、ユーザーに対し、顧客データを収納するアプリケーションまたはシステムへのアクセスに多要素認証を使用することを要求する。

10.1.3 シングルサインオンおよび多要素認証。 シングルサインオンおよび多要素認証は、権限を有する人物のみに進入を制限するようデザインされたすべての Tealium システムへのアクセスポイントで、進入する際に必要とされる。

10.2 セッション設定。 顧客データにアクセスするセッションは、最大 60 分ユーザーが操作しないとタイムアウトになるように設定される。かかるタイムアウトまたは操作のない時間経過後は、再認証が必要となる。

10.3 ログインの失敗回数。 ログインの試みの失敗回数は、最大 5 回に制限される。許される最大のログイン失敗回数を超えると、ユーザーアカウントは少なくとも 10 分間ロックされる。

10.4 遠隔アクセス。 顧客データを収納する Tealium システムの遠隔アクセスは、承認された

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:

ユーザーに限定され、多要素認証を必要とし、また検査のため記録される。

10.5 効力停止。 顧客データへアクセスできる Tealium の人員のユーザーID は、職務の変更に伴い当該アクセスが不要になった場合、または雇用が終了した場合には、直ちに効力を失う。

10.6 特権アクセス。 Tealium は、業界基準の方法により、以下を提供する。:

10.6.1 顧客データを収納する Tealium システムにアクセスできる Tealium のユーザーは、作業遂行のために必要最小限の特権を付与される。

10.6.2 特権アクセスは、権限を付与された個人ユーザーに制限され、否認防止は維持される。

10.6.3 特権ユーザーアカウントは、特権的操作のためにのみ使用され、通常活動としての事業には使用されない。

10.6.4 開発担当者は、Tealium システムの運営とサポートに必要な場合、管理された環境でのみ、限定的に生産環境への特権アクセスを付与されることがある。

10.6.5 すべての特権アクセスには、多要素認証が要求される。

11. ログ記録と監視。

11.1 Tealium のネットワークの監視。 Tealium は、顧客データが処理される本サービスをサポートする Tealium のネットワークを積極的に監視し、アクセス制御の方針からの逸脱、および実際の侵入もしくは侵入未遂、またはその他の不正行為を探知する。

11.2 イベントのログ記録。 Tealium システムによる顧客データの処理のため、Tealium は以下を行う。

11.1.1 顧客に提供される本サービスの秘密保持、

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 such 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

完全性、および・または利用可能性に影響を与える可能性がある」と合理的に判断され、かつ、Tealium システム上で発生しているセキュリティインシデントの特定または調査に役立ちうる重要なセキュリティイベント（アクセスイベントを含む）のログ記録を維持する。かかる該当するログ記録のコピーは、顧客の書面上の要請に応じて入手可能となる。

11.1.2 ログ記録を修正または削除から保護する、

11.1.3 定期的にログ記録を見直す、

11.1.4 業界基準の形式でログ記録を保存する、また

11.1.5 ログ記録を少なくとも 12 ヶ月間保管する。

12. ソフトウェアセキュリティに関する保証。

12.1 開発手法。 本サービス提供の過程において使用されるソフトウェアについて、Tealium は以下を実行する。

12.1.1 文書化された安全な SDLC に従って内部開発活動を実施する。顧客は、要求によりこれを共有することができる。

12.1.2 SDLC に厳格に従って、新しいアプリケーションおよび既存のアプリケーションの変更を現行の生産環境にデプロイする。

12.1.3 要件分析、システム分析、セキュリティ要件の定義付け、システムのデザイン、開発、統合およびテスト、変更許可、デプロイ、およびメンテナンスを含む、文書化された SDLC の手続きを維持する。

12.2 開発環境。 本サービス提供の過程において使用されるソフトウェアについて、Tealium は、生産環境から隔離され、かつ、不正開示から顧客データを保護する特別な環境下において、システム開発およびテストを行う。

12.3 容量および機能のプランニング

Tealium は、Tealium システム不良または停止の可能性および影響を最小限に抑えるようデザインされた、容量および機能のプランニングの手順に従う。Tealium は、定期的に容量プランおよび機能の監視情報を見直す。

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 Code 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.

<p>12.4 ソフトウェアセキュリティーテストプロセス。 本サービスの提供の過程において、Tealium は以下を実行する。</p> <p>12.4.1 アプリケーションが正式なコードレビュープロセスを受けるように設定する。 Tealium は、顧客から書面上の要求があった場合、正式なプロセス実行の証拠を顧客に提供する。</p> <p>12.4.2 アプリケーションがダイナミックアプリケーションセキュリティーテスト (DAST)、ソフトウェアコード構成分析 (SCA)、および静的アプリケーションセキュリティーテスト (SAST) を受けるように設定する。テストの採点および問題評価の方法は、アメリカ国立標準技術研究所 (「NIST」) が公表する最新の共通脆弱性評価システム (「CVSS」) など業界の慣行に従う。また</p> <p>12.4.3 アプリケーションが少なくとも年に一度、脅威モデル分析を受けるように設定する。Tealium は、脅威モデルについて正式に結果を報告しおよび重大な瑕疵を修復するプロセスを実行する。Tealium は、顧客の要求があった場合、脅威モデルの要旨を共有することにより、かかる活動を証明する。</p> <p>13. データセンターの管理。</p> <p>13.1 基本要件。 本サービスをサポートするすべてのデータセンターは、以下の最低要件を備えるものとする。:</p> <p>13.1.1 本 DSS セクション 6 および 7 に定める適切な物理的セキュリティーおよびアクセスコントロール</p> <p>13.1.2 業界基準の HVAC および環境管理</p> <p>13.1.3 業界基準のネットワーク/ケーブルの環境</p> <p>13.1.4 業界基準の冗長かつ大容量のネットワーク帯域</p> <p>13.1.5 専門的の火災探知/消火機能</p> <p>13.1.6 業界基準の無停電電源の供給 および</p>	<p>14. Business Continuity Plan (BCP).</p> <p>14.1 BCP Planning and Testing</p> <p>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</p> <p>14.1.2 Tealium will maintain processes for timely recovery of Services.</p> <p>14.2 BCP Plan. The plan will address the following additional standards or equivalent in all material respects:</p> <p>14.2.1 regulatory requirements and Industry Standards;</p> <p>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;</p> <p>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;</p> <p>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</p> <p>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.</p> <p>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</p>
---	---

<p>13.1.7 包括的事業継続プラン</p> <p>14. 事業継続プラン(BCP)。</p> <p>14.1 BCP プランおよびテスト</p> <p>14.1.1 Tealium のプランニング機能には、MSA に基づく Tealium の義務の履行に必要なすべてのハードウェア、ソフトウェア、通信機器、ならびにデータおよびファイルの現行のコピーをから成るデータ回復システムが含まれる。</p> <p>14.1.2 Tealium は、Tealium が所有する、または Tealium が運営するデータセンターにおいて本サービスの適時回復のプロセスを実行する。</p> <p>14.2 BCP プラン。 このプランは、すべての重要な点において、以下の追加的またはこれと同等の基準を示す。：</p> <p>14.2.1 当プランは、規制および業界慣行を反映する。</p> <p>14.2.2 Tealium の通常業務、システムおよびプロセスの中断、または損失が発生した場合に発生すると Tealium が確信し、予想する影響および効果の業務影響度の分析を含む。</p> <p>14.2.3 本サービス提供のため、および MSA に基づく Tealium の義務を履行するために Tealium が使用する主要な場所およびシステムと遜色のない能力を有する代替場所および代替システムの設立と維持。</p> <p>14.2.4 大事故発生後に実施される復旧手順の詳細であって、事業の継続を維持するために必要な、Tealium の事業運営、システムおよびプロセス、ならびに重要な人員、リソース、サービスおよび活動の復旧を確実にするための緊急時の準備の詳細を示すもの。</p> <p>14.2.5 大事故発生後に Tealium の事業運営、システムおよびプロセスが復旧する目標時間を示すスケジュール。Tealium は、復旧手順および BCM プランが、修復時間目標（「RTO」）を 4 時間、復旧時点目標（「RPO」）を 24 時間に設定することに同意する。</p>	<p>Customer of such disaster. Such notification will, as soon as such details are known, describe:</p> <p>14.3.1 The disaster in question and how it was detected;</p> <p>14.3.2 The impact the disaster is likely to have on the Services;</p> <p>14.3.3 The alternative operating strategies and the back-up systems Tealium will utilize and the timetable for their utilization; and</p> <p>14.3.4 The expected timeframe in which the disaster will be resolved and Tealium expects to return to business as usual.</p> <p>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.</p>
---	--

<p>14.3 通知。 MSA に基づく Tealium の義務遂行能力、または本サービスに影響が出ると Tealium が合理的に判断する大事故が発生した場合、Tealium は、当該大事故について速やかに顧客に通知する。かかる通知には、詳細が明らかになり次第、以下の事項が含まれる。</p> <p>14.3.1 問題の大事故の内容、およびどのように探知されたか</p> <p>14.3.2 大事故が本サービスに及ぼすと予想される影響</p> <p>14.3.3 Tealium が利用する代替運営方法およびバックアップシステム、ならびにそれらの利用のタイムテーブル</p> <p>14.3.4 大事故が解決し Tealium が通常業務に戻るのにかかると予測される時間</p> <p>14.4 サブプロセッサ。 Tealium は、本サービスのいずれか一部（本サービスを円滑にするための補助サービス（例えば、文書の倉庫保管および検索、プリントサービスなど）を除く）を提供するそのサブプロセッサが、取締役規定および業界の最良の慣行に従った、商業的に合理的な事業継続プログラムを準備し、維持することを要求する。Tealium によるサブプロセッサの利用は、サブプロセッサの出处および顧客への通知の有無にかかわらず、MSA に基づいて提供されるすべての本サービスのための、Tealium が事業継続可用性を提供する義務（上記に示される）を消滅させるものではない。</p>	
--	--

<p align="center">TEALIUM INC. データ処理補足条項 (補足条項 DPA)</p> <p>本データ処理補足条項(「DPA」)は、顧客による Tealium からの本サービスの購入に関する Tealium と顧客間の MSA、またはその他の、書面上あるいは電子上の、本 DPA を参照するサービス条件もしくは購入契約書(「MSA」)の一部を構成し、その対</p>	<p align="center">TEALIUM INC. DATA PROCESSING ADDENDUM (Addendum DPA)</p> <p>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</p>
---	--

象となる。本 DPA は、署名されたか、または参照により組み込まれたか否か（URL リンクを通じてなど）にかかわらず、すべての本書以前の契約書に優先する。

1. 定義。 本 DPA の目的のため、GDPR および CCPA で使用される語句と定義（ここに定義する）が適用される。さらに、MSA に別途定義されない限り、DPA で使用されるすべての大文字の語句は、以下に定められた意味を持つものとする。：

「**APPI**」とは、個人情報保護法（2020 年改定の 2003 年版法番号 57）をいう。

「**顧客データ**」は、MSA に定義される意味を持つ。

「**データエクスポート**」および「**データインポート**」は標準契約条項で与えられた意味を持つ。

「**データ保護法および規制**」とは、MSA に基づく個人データ処理時における各当事者の役割に適用される法律および規制を含む、個人データの機密性、完全性、処理および・または保護に関連するすべての法律および規制をいい、該当する場合、GDPR、プライバシー法、APPI、PIPEDA、米国プライバシー法が含まれる。

「**データセキュリティー規定**」または「**DSS**」とは、Tealium の技術的かつ組織的セキュリティー対策に関する規定をいう。

「**EEA**」とは、本 DPA の目的上、欧州経済領域および英国をいう。

「**GDPR**」とは、個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679 をいう。

「**無許可のデータ**」とは、その不正開示または不正使用により、データ対象の潜在的な重大なセキュリティーまたはプライバシーのリスクが合理的に発生するおそれがある個人特定可能な情報（国民保険番号、パスポート番号、運転免許証番号、もしくは類似の識別番号などの政府発行の識別番号、クレジットカード番号やデビットカード番号、医療または財務情報、生体情報、および／または財務、医療、あるいはその他のアカウント認証データ（パスワードや個人識別番号など）含むが、これらに限らない）をいう。

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

「**個人データ**」は、特定可能な個人に関する情報の収集、使用、保管または公開に関連した適用法または法令に定義された意味を持ち、かかる定義がない場合、特定の個人を識別し、連絡または所在地を確定するために使用されうる個人に関する情報、またはその他の情報と組み合わせることによって特定の個人を識別し、連絡または所在地を確定するための特定の個人に関連付けられる情報をいう。DPAの目的上、個人データは、添付書類2に記載のある「処理」の範囲に示される通りである。

「**PIPEDA**」とは、カナダ個人情報保護および電子文書法をいう。

「**プライバシー法**」とは、1988年オーストラリア連邦プライバシー法(Cth.)をいう。

「**処理すること**」または「**処理**」とは、顧客データに作動するオペレーションまたはオペレーションの集合体の一切（自動装置によるものか否かに限らない）をいう。その例として、閲覧、収集、記録、編成、構成、ストレージ、適合または変更、入手、参照、使用、送信による開示、流布またはその他の方法による公開、同調または結合、制限、消去または破棄などが挙げられる。

「**売却**」および「**共有**」は、CCPAに定義される意味を持つものとする。

「**サービスプロバイダ**」は、CCPAに定義される意味を持つものとする。

「**標準契約条項 (Standard Contractual Clauses)**」とは、(EU)2016/679規制に基づく、個人データの第三国への送信のための標準契約条項に関する、2021年6月4日採択の欧州委員会の実施決定の付属書、ならびに、該当する場合、英国版補填をいう。

「**セキュリティインシデント**」とは、顧客データの破壊、損失、変更、無許可の開示あるいは顧客データへのアクセスに繋がる、無許可または違法なセキュリティの侵害をいう。ただし未然のセキュリティ事故を除く。

「**Tealium システム**」とは、Tealium またはそのサブプロセッサの管理内にあり、かつ本サービスを提供するために使用される、データセンター、ネットワーク機器、アプリケーション、およびホストソフトウェアシステム（仮想ファイアーウォールなど）をいう。

「**英国補填**」とは、2018年データ保護法 S119A(1)

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.

に基づいて英国情報保護監督機関によって発行された、欧州委員会の標準契約条項の英国版補填をいう。

「**英国 GDPR**」とは、2018 欧州連合離脱法第 3 条によって、イングランド、ウェールズ、スコットランドおよび北アイルランドの法律の一部をなす GDPR をいう。

「**未然のセキュリティーインシデント**」とは、顧客データのセキュリティーの危殆化に至らない未然の試みまたは活動をいう。これには、ファイアウォールまたは端末サーバーへのピングおよびその他のブロードキャストの攻撃、ポートスキャン、未然のログインの試み、サービス攻撃の拒否、パケット盗聴（またはその他の、ヘッダーへのアクセスに至らないトラフィックへの無許可のアクセス）、もしくは同様のインシデントを含むがこれに限らない。

「**米国プライバシー法**」とは、カリフォルニア州消費者プライバシー法 §§ 1798.100 修正（「**CCPA**」）、随時修正または更新される、カリフォルニア州消費者プライバシー法パート 4 ディビジョン 3 タイトル 1.81.5 セクション 1798.100 およびそれ以下として成文化された、2020 年カリフォルニア州プライバシー権利法（「**CPRA**」）、および同様の米国州立プライバシー法または規制のすべてを含む、個人データの処理を統括するすべての米国州法いう。

「**ユーザーデータ**」は、MSA に定義される意味を持つ。

より詳しい定義は本 DPA を通じて示される。

2. データ処理。

2.1 範囲および役割。 本 DPA は、MSA に基づき本サービスを提供する過程において Tealium がデータプロセッサまたはサービスプロバイダーとして顧客を代表して個人データを処理する場合においてのみ適用される。

“**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 any 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

2.2 法への準拠。 Tealium は、MSA に基づく本サービスの受領過程において、自身に適用される、または自身に課されるすべてのデータ保護法および規制（データ保護に関するすべての法廷要件を含む）に準拠する。両当事者は、当 DPA 添付書類 1 に定義されるデータ保護法および規制に要求される追加義務に従う。

2.3 データ処理の指示。

2.3.1 Tealium は、顧客の文書化された指示を代表し、またそれにのみ従って個人データを処理する。これには、顧客の本サービスの設定、本サービスまたは SOW に含まれる指示、および・または本 DPA および MSA に含まれる指示を含むがこれに限らず、また第三国または国際組織への個人データの転送に関する事項が含まれるが、Tealium が対象となるデータ保護法および規制に要求される場合はこの限りでなく、その場合 Tealium は、処理を行う前に、顧客に該当する法律要件を通知しなければならない（かかる法が重要な公共の利益を理由に当該情報提供を禁止する場合を除く）。Tealium は個人データを販売せず共有しないことを保証する。

2.3.2 顧客は次の目的のために Tealium の個人データの処理を指示する。：(a) MSA に基づく処理、(b) 本 DPA に基づく処理、(c) 顧客の、MSA および DPA に抵触しない、合理的な書面上のあらゆる要求に基づく処理。特に、Tealium は、本サービスの実行という特別な目的のためにのみ、個人データを取得し、使用し、あるいは開示する。本 DPA を締結することによって、Tealium は契約上の制限を理解し、またこれに従うことを保証する。当セクション 2.4 の範囲外の処理については、かかる処理における追加指示に関して、Tealium と顧客間の事前の書面合意（Tealium が追加指示を実行する際にかかる追加費用の一切を、顧客が Tealium に支払う合意を含む）が必要となる。

2.3.3 ある指示がデータ保護法および規制のあらゆる条項に抵触していると Tealium が判断した場合、Tealium は顧客に直ちに通知しなければならない。その場合、顧客がかかる指示を確認するか、その指示を変更するまで、Tealium は指示に従う必要がないものとする。

2.4 開示。 Tealium は、MSA の条件によって明示的に許可される場合、ならびに適用法および規制あるいは法務執行機関の有効で拘束力のある命令（召喚命令や裁判所命令など）に従う必要がある場合を除いて、個人データを第三者に開示しない。法務執

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 2.4 (if any) will require prior written agreement between Tealium and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to Tealium for carrying out such instructions.

2.3.3 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

行機関が Tealium に個人データの開示命令を送った場合、Tealium は、法務執行機関が直接顧客に当該データの開示を再要求するよう試みる。この試みの一部として、Tealium は法務執行機関に顧客の基本連絡情報を提供することができる。法務執行機関に個人データを開示する必要がある場合、顧客が秘密保持命令またはその他の適切な救済を求めることができるよう、Tealium は顧客にかかる要求の合理的な通知をする（Tealium が法的に禁止される場合を除く）。Tealium は、最終審の管轄裁判所が開示に関する最終命令を発するまで、各当局に対し個人データの開示を回避する。要請があった場合、Tealium は顧客に、MSA に基づく個人データ処理に関して公的当局から受けた要請に関する一般的な情報を提供する（少なくとも要請回数、要整されたデータの種類、要請主体、機密保持義務のある要請の回数）。

2.5 ユーザーデータ。本サービスの一部として、Tealium は、(a) 権限のあるユーザーによる本サービスへのアクセスおよび使用を許可し Tealium と本サービスについて連絡を取り、また (b) Tealium の商品およびサービスの開発、改良、サポートおよび運営を実行するため、ユーザーデータを収集および使用する。

3. Tealium の人員。

3.1 秘密保持、信頼性、およびアクセスの制限。Tealium は、個人データを処理する権限を与えられた Tealium の人員が、秘密保持およびデータ保護とデータセキュリティーに関する関連義務を含む適切な契約的義務を果たすこと、またはかかる人員が適切な秘密保護の法定義務に拘束されていることを保証する。Tealium は、個人データの処理に携わる Tealium の人員の信頼性を保証するため合理的な措置を講じる。Tealium は、データセキュリティー規定に示される通り Tealium が承認しない限り、Tealium の人員による個人データの処理を制限する。

3.2 訓練。Tealium は、Tealium の人員が個人データに関する責務における適切な訓練を受けていることを保証する。

3.3 データ保護担当者。Tealium はデータ保護担当者を指定した。指定された担当者には、dpo@tealium.com から連絡することができる。

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. Tealium のセキュリティーの義務。 Tealium は、以下を実行する。:

4.1 最新鋭の技術水準、実装にかかる費用、処理の性質・範囲・コンテキストおよび目的、ならびに自然人の権利および自由に係る可変の可能性と重大性を考慮し、かかるリスクに見合ったレベルのセキュリティーを提供するためにデザインされた適切な技術的かつ組織的措置を講じる。かかる措置は、最低でも、データセキュリティー規定に定義される条件を満たす。

4.2 サブプロセッサの雇用において本 DPA セクション 9 に参照される条件を尊重する。

4.3 処理の性質を考慮し、本 DPA セクション 5 に示される通り、データ保護法および規制に基づく、データ主体の権利に関する要求に対する顧客の応答義務の履行のため、可能な限り、技術的かつ組織的措置によって顧客を補助する。

4.4 処理の性質および Tealium に開示された情報を考慮し、データ保護法および規制に基づく顧客の義務（処理時のセキュリティー、データ漏洩の通知、プライバシー影響評価、および監督当局への協力に関する義務）の履行を補助する。

1.1 インフラ、アプリケーション、関連する本サービスのセキュリティーを定期的に検証する。

Tealium の情報セキュリティープログラムの適性は、業界のセキュリティー基準、および Tealium の方針と手順への準拠に対して評価される。

Tealium は、Tealium のネットワークおよび関連する本サービスのセキュリティーを継続的に評価し、新しいセキュリティーの脅威、または定期的な審査によって明らかになる発見に対応するために、セキュリティーの措置の追加または緩和の必要性があるかどうかを決定する。Tealium は、継続的脆弱性のテストおよび年次の侵入テストによって、欠陥を検知し、また欠陥があった場合その修復を行う。Tealium のネットワークおよび関連する本サービスは、セキュリティーインシデントの発生または発生の可能性において継続的に監視される。Tealium はまた、少なくとも年に一度、または環境に重大な変化が起きた場合にリスク査定を行う。これらの措置は、情報セキュリティープログラムの継続的改良のために講じられる。

5. 顧客の制御権およびデータ主体の権利。

5.1 顧客の制御。 本サービスは、顧客が、個人データを取得し、修正し、削除し、もしくはブロックし、またデータ主体の要求（以下定義）に応答する

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

権限を与える。Tealium は、顧客が使用すると決めた場合に利用可能な、特定のセキュリティー機能と機能性を提供する。

5.2 データ主体の権利。 Tealium が、顧客に関連していると Tealium が知るところのデータ主体に要求を受けた際には、データ主体の（情報へ）アクセスする権利・改正する権利・処理の制限・削除（「忘れられる権利」）・データポータビリティ・処理の拒否・または自動処理による個人に関する決定を行使するため、Tealium は、法的に許される限りすみやかに顧客に通知する（「データ主体の要求」）。さらに、本サービスを使用している顧客がデータ主体の要求にアクセスできない場合、Tealium は、顧客の要請を受けて、データ主体の要求への顧客の回答を援助する。

6. 個人データの転送。

6.1 リージョン。 顧客は、Tealium システム内の個人データが静止状態でホストされる場所を特定することができる。ホストロケーションのリストは、Tealium によって随時更新される、Tealium のサブプロセッサのページで閲覧可能である（それぞれ「リージョン」という）。顧客が本サービス設定中リージョンをいったん決めると、顧客の追加指示なしに、または、セクション 2.5 に示される通り法律あるいは法務執行機関の有効で拘束力のある命令（召喚命令や裁判所命令など）に従う必要がある場合を除いて、Tealium は、顧客の選定したリージョンから静止状態の個人データのホストを転送しない。ユーザーデータは、米国にてホストされる。

6.2 標準契約条項の適用。 標準契約条項は、EEA、スイスまたは英国（該当する通り）圏外に、直接または第三者の送信を通じて、適切な水準の個人データの保護を提供すると欧州委員会、連邦審議会または英国省大臣（該当する通り）に認められていないその他の国々に送信される、個人データに適用される。Tealium が、GDPR/英国 GDPR 第 46 条に基づいて EEA、スイスまたは英国（該当する通り）圏外に個人データを合法的に送信するための、認識される代替遵守基準を採用した場合、標準契約条項は適用されない。

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

<p>6.3 セクション 6.2 に基づいて該当する場合、(i) 標準契約条項は本 DPA 添付書類 2 に示される通り適用され、また(ii) 標準契約条項は、相反する本 DPA の条件に優先する。</p> <p>6.4 データプライバシーフレームワーク。 Tealium は、欧州米国データプライバシーフレームワーク（「DPF」）に準拠し、DPF の原理に従う。 Tealium の証明書はここで閲覧できる。</p> <p>7. サティフィケーションおよび監査。</p> <p>7.1 Tealium の監査。 Tealium は、少なくとも年に一度、自身のプライバシーおよびセキュリティー対策の監査を行う。これらの監査は、ISO/IEC 27001、および SOC 2 タイプ II の基準、またはこれらの基準に実質的に同等の、その他の代替基準に基づいて行われる。これらの監査は、Tealium の選定と費用負担によって、第三者のセキュリティー専門家によって行われる。</p> <p>7.2 監査の報告。 顧客は、本 DPA に基づく Tealium の義務を果たしているかを合理的に検証することができるよう、Tealium の 監査報告書および認定証のコピーに、trust.tealium.com にてアクセスすることができる。かかる報告書は Tealium の本秘密情報を構成する。</p> <p>7.3 顧客の監査。 顧客の監査に関する権利は、DSS に定義される。</p> <p>8. セキュリティーインシデントの通知。</p> <p>8.1 Tealium の通知。 Tealium がセキュリティーインシデントを確認した場合、不当な遅延なしに、可能な場合、確認した時点から 48 時間以内に顧客にセキュリティーインシデントの通知をする。48 時間以内に顧客が通知を受けなかった場合、遅延の理由がなければならない。</p> <p>8.2 セクション 8.1 にある通知には少なくとも以下の点が含まれなければならない。:</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>7. Certifications and Audits.</p> <p>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.</p> <p>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.</p> <p>7.3 Customer Audits. Customer’s audit rights are as set forth in the DSS.</p> <p>8. Security Incident Notification.</p> <p>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.</p> <p>8.2 The notification referred to in Section 8.1 shall at least:</p> <p>8.2.1 describe the nature of the Security Incident;</p>
---	---

<p>8.2.1 セキュリティーインシデントの性質の説明</p> <p>8.2.2 データ保護担当者またはより多くの情報が得られるその他の者の氏名と連絡先の詳細、および</p> <p>8.2.3 Tealium がセキュリティーインシデントを是正するために講じた、または申し出た措置（悪影響が出る可能性がある場合、これを最低限に抑える適切な措置を含む）の説明。</p> <p>8.3 情報の同時提供が不可能な場合、過度の遅延なく、段階ごとに情報を提供することができる。</p> <p>8.4 Tealium は、あらゆるセキュリティーインシデント、セキュリティーインシデントに関する周辺事実、その影響および講じられた是正措置を文書化しなければならない。かかる文書は顧客が当セクションに遵守しているかを認めることができるものでなければならない。</p> <p>8.5 Tealium のサポート。 データ保護法および規則に基づいて顧客が要求される、あらゆる個人データ漏洩の通知に関して顧客をサポートするため、Tealium は、セクション 8.1 に基づき、Tealium が顧客に合理的に開示できる情報を通知に含む。その際 Tealium は、本サービスの性質、Tealium が知ることができる情報、および機密情報など情報開示のあらゆる制限を考慮する。</p> <p>8.6 未然のセキュリティーインシデント。 顧客は未然のセキュリティーインシデントが本セクション 8 に準拠しないことに合意する。:</p> <p>8.7 送達。 セキュリティーインシデントの通知は、email を含む、Tealium が選択するあらゆる合理的な方法によって、一人または複数の顧客の運営者に届けられる。Tealium に顧客の運営者の正しい連絡先を常に知らせておくことは、顧客の単独の責任である。</p> <p>8.8 責任。 当セクション 8 に基づく Tealium のセキュリティーインシデントの報告または対応の義務は、かかるセキュリティーインシデントに関する Tealium の過失または責任の一切を、Tealium が認めたことにはならず、将来的にもそうならないこと。</p> <p>9. サブプロセス。</p>	<p>8.2.2 communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>8.6 Unsuccessful Security Incidents. Customer agrees that an Unsuccessful Security Incident will not be subject to this Section 8:</p> <p>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.</p> <p>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.</p> <p>9. Sub-Processing.</p> <p>9.1 Authorized Sub-processors. Customer agrees that Tealium may use the sub-processors set forth at Tealium Sub-Processors Page to fulfill</p>
--	---

9.1 権限を付与されたサブプロセッサ。 顧客は、Tealium が本 DPA に基づく特定の契約的義務を果たすため、また Tealium を代表して特定のサービスを提供するため、[Tealium Sub-Processors Page](#) で定義されるサブプロセッサを Tealium が利用できることに同意する。Tealium は、サブプロセッサの追加または変更を意図する場合、顧客がその変更に関する異議を申し立てることができるよう、顧客にその意図を少なくとも 30 日前までに通知する。通知は適用されるウェブサイトに行われるアップデートを含み、顧客が当該アップデートの通知を受け取る設定を提供することがある。

9.2 サブプロセッサに関する義務。 当セクション 9 に示される通り、Tealium がサブプロセッサに権限を与える場合、Tealium は以下を実行する。:

9.2.1 Tealium は、サブプロセッサの個人データへのアクセスを、本サービスの維持または顧客に本サービスを提供するのに必要なアクセスのみに制限し、サブプロセッサによるその他のあらゆる目的のための個人データへのアクセスを禁止する。

9.2.2 Tealium は、サブプロセッサに、書面による、本 DPA と同等かそれ以上の保護力のある、適切な契約義務を課す。かかる契約義務は、秘密保持、データ保護、データセキュリティおよび監査の権利を含む関連した契約義務を含む。

9.2.3 Tealium は、本 DPA の義務の Tealium の履行、およびサブプロセッサの作為または不作為を原因とする、本 DPA に基づく Tealium の義務の違反の一切に、継続的に責任を持つものとする。

9.3 サブプロセッサへの異議。 顧客が、Tealium による新しいサブプロセッサの採用に対し、合理的な理由を持って異議を唱える場合、顧客は、Tealium の通知から 20 営業日以内に、すみやかに、Tealium にその旨書面通知しなければならない。顧客が新しいサブプロセッサに反対する場合、Tealium は、合理的な努力を払って、影響のある本サービスの変更を顧客に申し出るか、あるいは顧客に非合理的な負担をかけずに、反対された新しいサブプロセッサによる個人データの処理を避けるため、影響のある本サービスの顧客のコンフィギュレーションまたは使用の、商業上合理的な変更を推奨する。Tealium が、かかる変更を合理的な期間内（60 日を超えないものとする）に提供できなかった場合、顧客は、Tealium に書面通知することで、反対された新しいサブプロセッサの使用なしに Tealium が提供できなかった本サービスに関してのみ、本サービス注文書を解約することができる。顧客は、かかる解約され

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

た本サービスに関して、解約成立日後の期間分、前払いした料金を返金されるものとする。

10. 通知義務。 破産または債務超過の手続き上、または第三者による同様の措置の過程で、個人データが Tealium の処理中に没収対象になった場合、Tealium は、不当な遅延なしに顧客に通知する。Tealium は、不当な遅延なしに、かかる手続きにおけるすべての関連当事者（債権者や破産管財人など）に、かかる手続きの対象となる個人データの一切が、顧客の財産かつ責任範囲であり、また個人データは顧客の単独に処分されることを通知する。

11. DPA の解約。 本 DPA は、MSA の解約日の遅い方の日付、またはそれ以降 Tealium が個人データを保持し続ける期間まで有効である。

12. 顧客の個人データの返却および消去。 本サービスは、顧客に、いつでも、個人データの取得または消去のために使用されうるの制御権を付与する。MSA の解約日まで、顧客は、当セクションに従って取得された個人データのすべてを収集または削除することができる。顧客が、本サービスの利用を通じて自力で当該個人データの収集または削除ができなかった場合、Tealium は、顧客の書面上の要請により、顧客によるかかる収集または削除をサポートする。顧客が MSA の解約または終了を通知した場合、Tealium は本解約日から 90 日以内に取得された個人データを消去する。いかなる場合であっても、Tealium は、MSA の解約日から 180 日以内に取得された個人データを消去する。

13. 料金および費用。 法で許される限り、上記セクション 6.1 に従って、顧客は、自身のアカウントのコンフィギュレーション中に最初に選定したリージョンの変更を顧客が要請した場合に発生する、あらゆる費用と料金を負うものとする。

14. 非開示。 顧客は、本 DPA は公開されたものではなく、本 DPA がまた MSA の秘密保護の条項に基づく Tealium の本秘密情報を構成することに同意する。

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

<p>15. 抵触。 本 DPA で修正されない限り、MSA は有効に存続する。MSA と本 DPA に抵触がある場合、本 DPA の条件が優先する。</p>	<p>terms of this DPA will control.</p>
--	--

<p style="text-align: center;">DPA 添付書類 1 – 特定管轄条項</p> <p style="text-align: center;">オーストラリア</p> <p>以下の条項は、顧客から Tealium に送られる個人データの転送のすべてに適用される。当該転送の処理は、個々人の個人情報の保護を統括する現在有効なまたは将来有効になる法律に含まれる、1988 年プライバシー法（「本法」）および オーストラリアプライバシーの原則（「APPs」）に基づいて行われる（「オーストラリア個人データ」）。</p> <p>(a) Tealium は、当 DPA に従ってオーストラリア個人データを処理しなければならない。</p> <p>(b) 顧客は、本法/APPs に要求される通り、適切な通知を提供し適切な合意を得なければならない。</p> <p>(c) Tealium は、データセキュリティ規定のそれと一致する、オーストラリア個人データを保護するために作成された保護措置を実行しなければならない。</p> <p>(d) 両当事者は、権限のある法的当局によるすべての有効な要請に従わなければならない。</p> <p>(e) 顧客の要請を受けた場合、Tealium は顧客に、DPA セクション 12 と一致する、オーストラリア個人データを受け取る機会を与えなければならない。</p> <p style="text-align: center;">カナダ</p> <p>以下の条項は、顧客から Tealium に送られる個人データの転送のすべてに適用される。当該転送の処理は、個々人の個人情報の保護を統括する現在有効なまたは将来有効になる、随時修正または更新されるカナダ個人情報保護および電子文書法（「PIPEDA」）、および 同様のカナダの連邦または州の法規制に基づいて行われる（「カナダ個人データ」）。当該法規制下では、顧客はカナダ個人データの制御者となり、Tealium はカナダ個人データの処理者となる。</p>	<p style="text-align: center;">Appendix 1 of the DPA – Specific Jurisdiction Provisions</p> <p style="text-align: center;">Australia</p> <p>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”):</p> <p>(a) Tealium shall Process the Australia Personal Data in accordance with this DPA.</p> <p>(b) Customer shall provide adequate notice and obtain appropriate consents as required by the Act/APPs.</p> <p>(c) Tealium shall implement security measures designed to protect Australia Personal Data consistent with the Data Security Statement.</p> <p>(d) Both Parties shall comply with all valid requests made by competent legal authorities.</p> <p>(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.</p> <p style="text-align: center;">Canada</p> <p>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:</p>
---	--

- (a) Tealium は、当 DPA に従ってカナダ個人データを処理しなければならない。
- (b) 顧客は、PIPEDA に要求される通り、適切な通知を提供し適切な合意を得なければならない。
- (c) Tealium は、データセキュリティー規定のそれと一致する、カナダ個人データを保護するために作成された保護措置を実行しなければならない。
- (d) 両当事者は、権限のある法的当局によるすべての有効な要請に従わなければならない。
- (e) 顧客の要請を受けた場合、Tealium は顧客に、DPA セクション 12 と一致する、カナダ個人データを受け取る機会を与えなければならない。

日本

以下の条項は、顧客から Tealium に送られる個人データの転送のすべてに適用される。当該転送の処理は、個々人の個人情報の保護を統括する現在有効なまたは将来有効になる、随時修正または更新される個人情報保護法（2020 年改定の 2003 年版法番号 57）（「**APPI**」）、および同様の日本の政府または地方の法規制に基づいて行われる（「**日本個人データ**」）。当該法規制下では、顧客は日本個人データの制御者（「**PIC**」）となり、Tealium は PIC の指示の下個人データを処理する。

- (a) Tealium は、当 DPA に従って日本個人データを処理しなければならない。
- (b) 顧客は、APPI に要求される通り、適切な通知を提供し適切な合意を得なければならない。
- (c) Tealium は、データセキュリティー規定のそれと一致する、日本個人データを保護するために作成された保護措置を実行しなければならない。
- (d) 両当事者は、権限のある法的当局によるすべての有効な要請に従わなければならない。
- (e) 顧客の要請を受けた場合、Tealium は顧客に、DPA セクション 12 と一致する、日本個人データを受け取る機会を与えなければならない。

米国カリフォルニア

- (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

以下の条項は、顧客から Tealium に送られる個人データの転送のすべて、および CCPA に基づく Tealium による個人データの処理に適用される（「カリフォルニア個人データ」）。ここでは、顧客は個人データに関する事業であり、Tealium はカリフォルニア個人データのサービス提供者である。

- (a) Tealium は、顧客が、本サービスを受ける限定的かつ特定の目的のためにのみ MSA に関連してカリフォルニア個人データを開示することを認める。
- (b) Tealium は、本サービスを提供するという特別な目的のため、またはその他法に基づいて必要な場合において、顧客を代表してのみ、カリフォルニア個人データを取得し、使用し、開示し、または処理しなければならない。Tealium によるカリフォルニア個人データの処理は、常に、MSA および本 DPA に準じて行われなければならない。
- (c) Tealium の以下の行動を禁ずる。
 - i. 本サービスの提供または法に基づいて必要な場合を除き、カリフォルニア個人データを取得し、使用し、開示し、または処理すること。
 - ii. カリフォルニア個人データを売却すること。
 - iii. カリフォルニア個人データを共有すること。
 - iv. 両当事者の直接的業務関係外でのあらゆる方法においてカリフォルニア個人データを処理すること。
 - v. その他のあらゆる第三者から受け取る、またはその第三者を代表して受け取る個人情報を、カリフォルニア個人データと組み合わせること。ただし、顧客に指示された場合、あるいは CCPA により明示的に許可された場合、Tealium はカリフォルニア個人データを事業目的のために組み合わせることができる。
- (d) Tealium は、データセキュリティ規定の監査に関する条項に則った、あらゆる合理的かつ適切な監査に協力することに同意する。Tealium は、CCPA、または MSA あるいは本 DPA に基づく義務に従うことができなくなった場合、直ちに顧客に書面通知することに同意する。本サービスの下請けのすべては本 DPA に定義される。Tealium は、顧客に協力し、CCPA に基づいて顧客に付与される権利を行使するための、証明可能な顧客の要請に応えこれを実行すること（DPA により詳しく定義される、適切な技術的および組織的措置を用いた補助を含む）に同意

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

<p>する。カリフォルニア個人データの削除は DPA に定義される。</p>	<p>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.</p>
--	---

<p style="text-align: center;">DPA 添付書類 2 処理の範囲</p> <p>本添付書類 2 の目的上、顧客はデータエクスポータであり、Tealium はデータインポータである。</p> <p><i>個人データが送信されるデータ対象者のカテゴリー</i> データ出力者は Tealium のサービスに個人データを提供することができる。その範囲は、エクスポータの単独の裁量により決定されかつ統制され、また以下のデータ対象クラスに関連する個人データを含みうる。(a)データ出力者のウェブサイト、モバイルアプリケーション、またはその他デジタルあるいは物理的プロパティへの訪問者、(b)データエクスポータによって個人データを本サービスにアップロードされるその他の人物、(c)データ出力者の従業員または代表者でありかつ本サービスのユーザー。</p> <p><i>送信された個人データのカテゴリー</i> データエクスポータは上記のデータ対象者に関する個人データを Tealium のサービスに提供することができる。その範囲は、データエクスポータの単独の裁量により決定されかつ統制される。データエクスポータは、データインポータが、本サービス内で処理されるデータのタイプを監視せず、それに通常無自覚であることを認める。</p> <p><i>送信される極秘データ</i> データインポータは、高機密データの処理の禁止を含む、本契約書の制限に従って、処理される個人データの範囲を決定し、また統制する。</p> <p><i>送信の頻度</i> 続く</p> <p><i>処理の性質</i> データインポータは、データエクスポータの指示および本サービスの設定に従ってデータ処理が行われるプラットフォームをホストする。</p> <p><i>データ送信の目的および後続処理</i> データインポータによる個人データの処理の目的</p>	<p style="text-align: center;">Appendix 2 to the DPA Scope of Processing</p> <p>For purposes of this Appendix 2, Customer is the data exporter and Tealium is the data importer.</p> <p><i>Categories of data subjects whose personal data is transferred</i> 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.</p> <p><i>Categories of personal data transferred</i> 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.</p> <p><i>Sensitive data transferred</i> Data exporter determines and controls the scope of personal data Processed subject to limitations in the MSA, including those relating to Prohibited Data.</p> <p><i>The frequency of the transfer</i> Continuous</p> <p><i>Nature of the processing</i> The data importer hosts the platform where data processing is carried out in accordance with data exporter’s instructions and configuration of the Services.</p> <p><i>Purpose(s) of the data transfer and further processing</i></p>
---	---

<p>は、MSA に基づく本サービスのパフォーマンスである。</p> <p>個人データが保持される期間、または不明な場合、かかる期間の判定基準</p> <p>本契約書の期間中、またはユーザーインターフェイスを通じて本サービスの設定中随時データエクスポータによって指定される期間。</p>	<p>The purpose of the Processing of personal data by data importer is the performance of the Services pursuant to the MSA.</p> <p><i>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period</i></p> <p>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</p>
---	--

<p align="center">DPA 添付書類 3 標準契約条項の適用</p>	<p align="center">Appendix 3 to the DPA Application of the Standard Contractual Clauses</p>
<ol style="list-style-type: none"> 1. 条項 7 は適用される/適用されない。 2. 条項 9(a) に関して、オプション 2 (一般書面許可書) が適用される。期間は 30 日とする。 3. 条項 11¹に関して、オプションが適用される/適用されない。 4. 条項 17²に関して、オプション 1 が適用される。メンバー州は、メンバー州は、データ対象者が所在するメンバーの州である。 5. 条項 18(b) に関して、メンバー州は、メンバー州は、データ対象者が所在するメンバーの州である。 6. 条項の付属書に関しては、 <ol style="list-style-type: none"> A. 当事者のリスト <p>データエクスポータは : DPA および MSA に「顧客」として示される事業体 これらの条項に基づいて送信されたデータに関連するアクティビティ : Web サービスへのアクセスおよび使用 役目(制御者/処理者): 制御者 理者</p> 	<ol style="list-style-type: none"> 1. Clause 7 shall/shall not be applicable. 2. With respect to clause 9(a), Option 2 (General written authorization) will apply. The time period is to be 30 days. 3. With respect to clause 11³, the Option shall/shall not be applicable. 4. With respect to clause 17⁴, Option 1 shall apply. The Member State is The Member State is the Member State where the data subject is located. 5. With respect to clause 18(b) the Member State is The Member State is the Member State where the data subject is located. 6. With respect to Annex I to the Clauses: <ol style="list-style-type: none"> A. LIST OF PARTIES <p>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 Processor</p>

¹ [オプション:データ出力者は、データ対象者が、データ対象者に無料で独立紛争解決機関に苦情を申し立てることもできることに同意する。]

² [オプション 1:これらの条項は EU メンバー州の一つの法律に統括される。ただしかかる法律は第三者の受益者の権利を認める。両当事者は_____ (メンバー州を記入) の法律であることに同意する。]

<p>データインポータは: Tealium Inc., 9605 Scranton Rd. Suite 600, San Diego, CA 92121, USA これらの条項に基づいて送信されたデータに関連するアクティビティ: Web サービスの条項 役目 (制御者/処理者): 処理者</p> <p>B. 送信の詳細</p> <p>添付書類 2 にて定義</p> <p>C. 権限のある監督当局</p> <p>権限のある監督当局はデータ対象者の所在地に所在するものである。</p> <p>7. 条項の付属書 II に関して、データインポータによって実施される技術的および組織的措置の記載は、データセキュリティ規定に定義される通りである。</p> <p>8. 本サービスの提供がスイスからの個人データの送信を含む場合、両当事者は、以下の変更を伴う本 DPA に組み込まれる標準契約条項に同意する。</p> <p>(a) 「2016/679 (EU) 規制」の参照は、スイス連邦データ保護法 (「FDPA」) の参照とみなされ、「2016/679 (EU) 規制」の特定の条文の参照は、FDPA の同等の条文またはセクションの参照であるとみなされる。</p> <p>(b) 「EU」「連合」および「メンバー州」の参照は、スイスの参照と置き換えられる。</p> <p>(c) 「権限のある監督当局」は、スイス連邦データ保護情報コミッショナーである。</p> <p>(d) 条項 17 では、EU SCCs はスイス法に統括される。</p> <p>(e) 条項 18(b) では、紛争はスイスの裁判所にて決議される。</p>	<p>The data importer is: Tealium Inc., 9605 Scranton Rd. Suite 600, San Diego, CA 92121, USA Activities relevant to the data transferred under these Clauses: Provision of web services Role (controller/processor): Process or</p> <p>B. DESCRIPTION OF TRANSFER</p> <p>As set forth in Appendix 2</p> <p>C. COMPETENT SUPERVISORY AUTHORITY</p> <p>The Competent Supervisory Authority is the one located where the data subject is located.</p> <p>7. With respect to Annex II to the Clauses, the description of the technical and organizational measures implemented by the data importer is as set forth in the Data Security Statement.</p> <p>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:</p> <p>(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;</p> <p>(b) references to "EU", "Union" and "Member State" shall be replaced with references to the Switzerland;</p> <p>(c) the "competent supervisory authority" shall be the Swiss Federal Data Protection and Information Commissioner;</p> <p>(d) in Clause 17, the EU SCCs shall be governed by the laws of Switzerland; and</p> <p>(e) in Clause 18(b), disputes shall be resolved before the courts of Switzerland.</p>
--	---