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 の顧客保護のパッケージ (「CPP」) 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 のデータ処理の方針の詳細が含まれます。

SLA

Tealium 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を提供します。Tealium は、稀ではありますが、ご利用できない状態になった場合の救済、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 がお客様のすべての問題に十二分に対応できると確信しています。

DSS

DSS は顧客データのためのセキュリティープログラムが示されます。これはすべてのお客様に平等

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 ("CPP") which are 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 policies in compliance with applicable privacy laws and regulations.

SLA

Tealium provides a website that provides real-time status, as well as notifications for maintenance and emergency outages. We provide remedies in the unlikely event that we miss this availability, 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 one customer. We are confident that our SLA will more than address all our customers' issues.

DSS

Our DSS reflects our security program for Customer Data, which applies to all of our customers equally. Please bear in mind that we do not access Customer Data except as required for

に適用されます。我々は、サポートのリクエストなど特別な目的のために必要な場合を除いて、顧客データにアクセスすることがないことにご留意ください。

以下の特別な理由により、お客様の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。

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になります。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。
2. Tealium は、通常は顧客データの内容を実際に見ることができません。Tealium が見ることのできないデータの内容には、データの匿名性、個人情報または秘密情報か否か、アカウント内の顧客データの特定の保存または構成の方法、 誰にデータが送られたか、データ処理の目的、処理の目的や量、データ送信先である第三者、およびあるデータまたは処理方法がデータの対象者にリスクを課すか否か（またはその程度）が含まれます。結果として、データのどの部分が業界特有の、または国特有の規定に準拠すべきなのかを判断するために必要な情報も、我々が見ることはできません。
3. Tealium の統一された厳格なセキュリティー制御は、すべてのお客様にとって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。我々の HIPAA に準拠した環境下で提供されるサービスによって、 セキュリティー保護対策が強化されています。これらの環境は第三者によって独自に評価され、米国 HIPAA 規定準拠の認証を伴って提供されています。

DSS はすべての商品とお客様に同様に提供されているため、個々のお客様のために DSS を変更する

a particular purpose (e.g., a support request).

There are specific reasons why we must use our DSS instead of using the data security documentation 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 data) differently from other customers.
2. Tealium generally has no visibility into the content of Customer Data, including whether or not it is pseudonymized, personal or sensitive, the particular manner in which you store or structure that Customer Data in your account, to whom the data relates, the purposes for which you process the data, the scope/volume of your processing, third parties you transmit the data to, and whether (or the degree to which) the particular data and/or processing poses risks to data subjects. As a result, we also will not have visibility necessary to determine which portions of the data may be subject to industry-specific or country-specific regulations.
3. All 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. Services provided in our HIPAA-compliant environments have enhanced security measures. These environments have been independently evaluated by a third party and provided with an attestation of compliance with the US HIPAA regulations.

Since our DSS is being provided uniformly across all our products and customers, we are unable to alter our DSS for one customer. We are confident that our DSS will more than address all our customer’s security issues. Note that while there is no customized offering, you are able to select the particular geographic hosting location(s) for

ことはできません。我々は DSS がお客様のすべてのセキュリティーに関する問題を網羅していると確信しています。カスタマイズされたサービスは提供できませんが、お客様のアカウントの 地理的なホストロケーションをお選びいただけます（MSA に詳細を定義）。	your account, as further defined in the MSA.
データ処理補足条項(「DPA」)	**The Data Processing Addendum ("DPA")**
DPA は、お客様が本サービスにアップデートするすべての個人データ（顧客データの一部）をカバーします。DPA は本サービスで処理される個人データのプライバシー保護対策を反映し、適用されるデータ保護法に基づく各当事者の特定の義務を示します。適用される場合、DPA はまた、欧州連合規制 2016/679 (「GDPR」)、1988 年オーストラリア連邦プライバシー法 (Cth.)、個人情報保護法（2003 年版法番号 57 の 2020 年修正）、およびカリフォルニア州消費者プライバシー保護法 §§ 1798.100 修正(「CCPA」)の追加条件など適用される米国プライバシー法の追加条件に言及します。我々の DPA には二つの異なるバージョンがあることに留意してください。お客様が欧州で事業を運営される場合、 標準的な契約条項を含む GDPR 版を要請するようお願いいたします。	The DPA covers all personal data (a subset of Customer Data) you upload to our Services. Our DPA reflects our privacy program for personal data we process in the Services and addresses certain obligations each respective party has under applicable data protection laws. Where applicable, our DPA also addresses additional requirements of the European Union's Regulation 2016/679 ("GDPR"), the Australian Privacy Act 1988 (Cth.), the Act on the Protection of Personal Information (act No.57 of 2003 as amended in 2020), and applicable US privacy laws such as the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. as amended ("CCPA"). Please note that we have two versions of our DPA. If you operate in Europe, please make sure that you request the GDPR version which includes the standard contractual clauses.
DPA は、 GDPR 28(3)および 46 の条項を含む、適用法の条件を満たすために特別に作成されました。 我々はお客様の顧客データにアクセスできず、またその内容を見ることができないため、プライバシーに関する適用法の条件が満たされているかの判断において、お客様が重要な役割を担っています。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個人データに対する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になります。	We drafted our DPA specifically to satisfy the requirements of applicable data protection laws, including those of Articles 28(3) and 46 of the GDPR. Because we do not have access or visibility to your Customer Data, you play an important role in how some of the requirements of applicable privacy laws 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 our Services meet requirements applicable to your particular personal data.
DPA はすべての商品とお客様に同様に提供されているため、個々のお客様のために DPA を変更することはできません。我々は DPA がお客様のすべてのセキュリティーに関する問題（適用法の準拠の可否を含む）を十二分に網羅していると確信しています。	Since our DPA is being provided uniformly across all our products and customers, we are unable to alter our DPA for one customer. We are confident that our DPA will more than address all our customers' privacy issues, including addressing compliance under applicable laws.

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

Service Level Agreement (SLA)

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

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

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

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

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

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

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

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

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

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

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 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

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。	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. 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。	**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. 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は商業的に道理的な努力を払い、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。	**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 excludedfrom the Availability.

DATA SECURITY STATEMENT (DSS)	データセキュリティー規定(DSS)
This Data Security Statement ("DSS") is incorporated into, and made a part of, the MSA between Tealium and Customer.	本データセキュリティー規定(「DSS」) は、Tealium と顧客間の MSA に組み込まれ、その一部となる。
General. Tealium will implement and maintain logical and physical security controls with respect to its access, use, and possession of Customer Data. These controls are designed to provide appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration, unauthorized disclosure 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 Network. 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.	**一般。** Tealium は、顧客データに対するそのアクセス、利用および保有に関し、論理的で物理的なセキュリティー制御を実行し、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 のネットワークの継続的機密性、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ー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。
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.	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異議を唱える機会を与える。
Definitions.	**定義。**
"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.	**「ダイナミックアプリケーションセキュリティーテスト」**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、そのセキュリティー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ーテストをいう。
"Encryption" means the process of using an algorithm to transform data into coded information in order to protect the confidentiality of the data.	**「暗号化」**とは、データの機密性を保護するため、データをコード化された情報に変換するアルゴリズムを用いたプロセスをいう。
"Firewall" means an integrated collection of security measures used to prevent unauthorized electronic	**「ファイアウォール」**とは、ネットワークコネクショ

access to the Tealium Network by implementing predetermined security rules for network communication.	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 のネットワーク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ー措置の集合体をいう。
"Industry Standards" means customs and practices followed by, and representing the degree of skill, care, prudence and foresight expected from leading providers of the types of services that are the subject matter of the MSA.	「**業界基準**」とは、MSA が対象とする種類のサービスの主要な供給者たちが遵守している慣習および慣行であって、当該主要な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。
"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.	**「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。
"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.	**「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。
"Malicious Code" has the meaning set forth in the MSA.	**「悪意のあるコード」**は、MSA に定義された意味を持つ。
"Multifactor Authentication" means authentication using at least two (2) 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.	**「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。
"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.	**「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ーテストをいい、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。
"Processing" or **"Process"** means any operation or set of operations which is performed on Customer Data, whether or not by automated means, such as viewing, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	**「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。
"Removable Media" means any portable or removable data storage device.	**「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データ保存メディアをいう。
"SDLC" means Secure Software Development Lifecycle Methodology, a documented process for	「**SDLC**」とは、情報セキュリティー対策（特にデザイン、テスト、および開発の工程時の対策）を必要とす

planning, creating, testing, and deploying, and/or delivering, an information system that requires information security engagement, particularly with respect to the design, test, and deployment stages.	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。
"Security Incident" means any breach of Tealium's obligations under this DSS that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, but does not include any Unsuccessful Security Incident.	「**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。
"Separation of Duties" means dividing roles and responsibilities so that a single individual cannot subvert the security controls of a critical process.	**「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。
"Source Code Composition Analysis" or **"SCA"** means a security test to identify open-source software, and any known security vulnerabilities in that software, in a codebase.	**「ソースコード構成分析」** または**「SCA」**とは、オープンソースソフトウェアおよびかかるソフトウェアの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。
"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.	「**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。
"Tealium Facilities" or **"Facilities"** means all Tealium owned or operated locations where Tealium personnel work and use Tealium Network and/or where Customer Data is Processed.	「**Tealium の施設**」または「**施設**」とは、Tealium の職員が勤務し Tealium のシステムを使用する場所、および/または、顧客データが収納されるまたは処理される Tealium のネットワークを使用する、Tealium が所有するまたは業務運営するすべての場所をいう。
"Tealium Network" means the data center facilities, servers, networking equipment, and host software systems (e.g. virtual firewalls) that are within the control of Tealium or its sub-processors and are used to provide the Services.	「**Tealium のネットワーク**」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、データセンター施設、ネットワーク環境、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。
"Threat Model" means a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view. The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.	**「脅威モデル」**とは、仮定の攻撃者の見地から潜在的な脅威を特定し、列挙し、優先順位をつけることができるプロセスをいう。脅威モデルの目的は、潜在的攻撃者のプロフィール、最も可能性の高い攻撃経路、および攻撃者が最も欲する資産について、防御者に体系的分析を提供することである。
"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-	「**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

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.	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。
"Root Cause Analysis" means a principle-based, systems approach for the identification of the underlying causes associated with a security event.	**「根本原因分析」**とは、セキュリティーイベ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. Incident Management and Security Incident Notification.	**3. インシデント管理およびセキュリティーインシデントの通知**
3.1 Incident Management. Tealium maintains a documented incident management policy and process to detect security events, and which provides coordinated response to threats and Customer notification. The process includes a Root Cause Analysis with identified issues tracked to remediation, and evaluation and implementation of actions to prevent recurrence.	**3.1 インシデント管理。** Tealium は、セキュリティー上の問題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続を整備し、脅威および顧客からの通知に対し連携した対応をとる。手続には、特定された問題の修復に至るまでの追跡を含む根本原因分析、ならびに再発を防ぐための措置の評価および実行を含む。
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 セキュリティーインシデントの通知と是正。** セキュリティー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ーインシデントを是正する。:
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.	**3.2.1 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、当該遅延の理由が提供されなければならない。
The notification shall at least:	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) describe the nature of the Security Incident;	**(1)** セキュリティーインシデントの性質の説明、
(2) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; and	**(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) 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.	**(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。
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.	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 shall document any Security Incidents, comprising the facts relating to the Security Incident, its	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

effects and the remedial action taken.

3.2.2 Root Cause Analysis. Tealium will promptly initiate and pursue to completion as quickly as possible a Root Cause Analysis.

3.2.3 Remediation. Tealium will promptly implement measures necessary to restore the security of Customer Data and Tealium Network. If such measures include temporarily restricting access to any information or Tealium Network 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. Service Organization Reports. Tealium will undertake at least annually, at its expense, an audit in accordance with ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 27701, and with the System and Organization Controls (SOC) Report under the SSAE-18 ("SOC 2") or their successor standard(s), covering controls related to Tealium's provision of the Services as a services organization, the scope of which will be in accordance with Industry Standard practice. In addition, Tealium will maintain TISAX Level 1 certification.

4.2. Third-Party/Subcontractor Agreements. Tealium will conduct a detailed risk assessment on its service providers who process Customer Data with results documented and made available to Customer upon written request.

4.3. Security Testing. Tealium will, at least annually, engage, at its expense, a third-party service provider to perform Penetration Testing of Tealium Network related to the provision of Services. 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

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。

3.2.2. 根本原因分析。 Tealium は本原因分析をすみやかに開始し、できるだけ早期の完了を目指す。

3.2.3. 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。

3.2.4. 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 サービス組織に関する報告。 Tealium は、少なくとも年に一度、自己の費用負担で、ISO/IEC 27001、ISO/IEC 27018、ISO/IEC 27701、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、監査を実施する。当該監査は、サービス組織としての Tealium の本サービスの提供に関連する管理体制をカバーするものとし、その範囲は業界基準の慣行に従うものとする。さらに、Tealium は TISAX レベル 1 の認定証を維持する。

4.2 第三者/ 下請業者の契約。 Tealium は、顧客データを処理する Tealium のサービス業者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。Tealium は、少なくとも年に一度、自己の費用負担で、第三者サービス業者に委託して、本サービスの提供に関する Tealium システムの侵入テストを行わせる。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。

of Standards and Technology ("NIST"). Tealium will remedy any validated findings deemed material (critical, high or medium risk) in a timely manner following such findings.

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 such other alternative standards as are substantially equivalent to SOC 2 or the 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 such other alternative standards which are substantially equivalent to SOC 2 or ISO/IEC 27001; and (c) will be performed by independent third-party security professionals.

4.5. Customer Audits (No Penetration Testing). Customer may conduct, either itself or through a third-party independent contractor selected by Customer at Customer's expense, an audit of the Tealium Facilities and procedures used in connection with the Services. Such audit shall be conducted no more frequently than one time per year, with 30 days' advance written notice unless required to comply with applicable laws and regulations or following a Security Incident affecting Customer Data. Any audits described in this Section shall be conducted during reasonable times, shall be of reasonable duration, shall not unreasonably interfere with Tealium's day-to-day operations, and be conducted in accordance with appropriate technical and confidentiality restrictions. In the event that Customer conducts an audit through a third-party independent contractor, such independent contractor shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the MSA to protect Tealium's Confidential Information. Customer must promptly provide Tealium with all information and reports in an unredacted format regarding any vulnerabilities or non-compliance discovered during the course of an audit.

4.6. Customer Audits (With Penetration Testing). In addition to the procedure set forth in Section 4.5 above, in case an audit includes Penetration Testing, such test shall be coordinated with Tealium's information security team and performed in a non-production environment running software with identical functionality to the

Tealium は、重大（危機的、優先度の高い、またはハイリスク）とみなされる発見があった場合には、当該発見の後、適時にこれを是正する。

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ー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ー対策の適性を検証する。そのセキュリティーは、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ーを含む。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ー専門家によって行われる。

4.5 顧客の監査（侵入テストを除く）。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、本サービスに関連して使用される Tealium のネットワークおよび手続きの監査を行うことができる。かかる監査は、多くて年に一度、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ー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基づいて行われなければならない。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 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、Tealium に、監査の過程で発見されたあらゆる脆弱性または違反に関するすべての情報と報告書を、無修正で、すみやかに提出しなければならない。

4.6 顧客の監査（侵入テスト）。 前述のセクション 4.5 に加え、ある監査が侵入テストを含む場合、当該テストは、Tealium の情報セキュリティーチームと協力して、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。

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 (8 am to 5 pm PST). PenTest environments shall only be scaled to the function of the test and not to a production scale.	PenTest は、 Tealium の通常営業時間（太平洋時間で午前 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。
5. Security Function.	**5 セキュリティー機能。**
5.1 Security Officer. Tealium will designate a point of contact to coordinate the continued security of all Customer Data and Tealium Network**.** The Tealium Security Officer can be contacted at infosec@tealium.com.	**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 ネットワーク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、infosec@tealium.com で連絡をすることができる。
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 regarding Tealium's processes for which compliance is required under the MSA, including, without limitation, procedures to verify all Tealium personnel promptly report actual and/or suspected Security Incidents. All personnel involved in any part of Tealium's SDLC are required to receive application security training. Tealium will retain documentation that such training has been completed.	**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、MSA の遵守が要求される Tealium のプロセスに関する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（この中には、Tealium の人員が実際のセキュリティーインシデントおよび/またはセキュリティーインシデントの恐れをすみやかに報告することを確認する手続が含まれるが、これに限定されない）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、アプリケーションセキュリティー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. Data Management. The following will apply to the Tealium Network that Processes Customer Data:	**6 データの管理。** 顧客データを処理する Tealium のネットワークには、以下が適用される。:
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 practices and secure all communications involving Customer Data access.	**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り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 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).	**6.2. 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、処理し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 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 Cryptographic Key Management. Tealium will securely manage cryptographic keys using secure key management systems and maintain documented	**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

Industry Standard control requirements and procedures for encryption key management.	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 Removable Media. Tealium does not use Removable Media in providing the Services.	**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 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.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、:
6.5.1 Tealium will maintain documented policies and procedures concerning data retention and disposal that include provisions to maintain chain of custody; and	**6.5.1.** 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、
6.5.2 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).	**6.5.2.** 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 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.	**6.6.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 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, 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.	**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、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。
7. Physical Security – Facilities. Tealium Facilities 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. At a minimum, all Tealium Facilities are required to have the following security-related characteristics:	**7 物理的なセキュリティー – 施設。**Tealiumの施設は、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。すべてのTealiumの施設は、少なくとも、以下の警備関連の特性を備えなければならない。:
7.1 Tealium will document, implement and maintain administrative and physical security policies, including, without limitation, a “clean desk” policy.	**7.1** Tealiumは、人的および物理的警備方針を文書化し、実行し、維持する。この中には、「クリーンデスクポリシー」が含まれるが、これに限定されない。
7.2 Tealium will install closed-circuit television (“CCTV”) systems and CCTV recording systems to monitor and	**7.2** Tealiumは、Tealiumの施設へのアクセスを監視し、記録するために、有線テレビ（「CCTV」）システムおよびCCTV録画システムを備え付ける。

record access to Tealium Facilities.

7.3 All Tealium personnel will be issued and will display an identification badge allowing electronic verification of the bearer's identity in order to gain access. Logs must be retained for at least one (1) year.

7.4 Each location will maintain procedures for validating visitor identity and authorization to enter the premises, including but not limited to, an identification check, issuance of an identification badge or escorted, validation of host identity, the purpose of visit, and recorded entry.

8. Tealium Network Security.

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

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

8.3 Intrusion Detection System. Intrusion Detection Systems will run on individual hosts or devices on the Tealium Network to monitor the inbound and outbound connections and will alert administrators if suspicious activity is detected. IDS will monitor file integrity of the Tealium Network 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 the Tealium Network providing or supporting Services to Customer, and such

7.3 すべての Tealium の人員には個人認証バッジが発行され、それを表示することにより、施設に入る際に所持者の身分証明の電子認証を受けられるようにする。記録は、少なくとも 1 年間は保管されなければならない。

7.4 各施設所在地は、訪問者の本人確認および施設への入場許可のための手続を維持する。この中には、身分証明の確認、認証バッジの発行、バッジ所持者の本人確認、訪問の目的および出入の記録が含まれるが、これらに限らない。

8 Tealium ネットワークセキュリティー。

8.1 資産目録。 Tealium は、現行の Tealium のネットワークのコンポーネント、ハードウェアおよびソフトウェア（バージョン番号および物理的所在地を含む）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 のネットワーク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ー。 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 のネットワーク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ーが検知されると管理人に警告する。IDS は Tealium のネットワーク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 のセキュリティー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、 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

tools are updated to provide protection against current threats.	またはその他の電子送信によって実施する。セキュリティーツールは、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 Vulnerability Management. Tealium will have a documented process to identify and remediate security vulnerabilities affecting Tealium Network containing Customer Data. Tealium will remediate identified and validated security vulnerabilities within a reasonable amount of time.	**8.5 脆弱性の管理。**Tealiumは、顧客データを収納するTealiumのネットワーク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。Tealiumは、発見されまた確認されたすべてのセキュリティー脆弱性を、合理的な時間内に修復する。
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.	**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. Change and Patch Management.	**9 変更およびパッチ管理。**
9.1 Change Management. Changes to applications, any part of Tealium's information technology infrastructure, and/or the Tealium Network will be tested, reviewed, and applied using a documented change management process and adhere to the principle of Separation of Duties.	**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のネットワークの変更は、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 Emergency Changes. Tealium uses an emergency change approval process to implement changes and fixes to the Tealium Network and Services on an accelerated basis when necessary. Tealium will notify Customer in advance if any such emergency changes could affect the functionality of Services.	**9.2 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のネットワーク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 Software Updates. Tealium will:	**9.3 ソフトウェアのアップデート。** Tealiumは、:
9.3.1 use security software in support of the delivery of Services;	**9.3.1** 本サービスの提供のため、セキュリティーソフトウェアを使用し、
9.3.2 use only supported versions of software required for the delivery of Services; and	**9.3.2** 本サービス提供に必要なソフトウェアは、サポートされるバージョンのみを使用し、
9.3.3 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.	**9.3.3** 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. Logical Access Controls.	**10 論理的なアクセスコントロール。**
10.1 User Authentication: Tealium will implement processes designed to authenticate the identity of all	**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。**:**

users through the following means**:**	**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。Talium 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。
10.1.1 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 Network 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**.**	**10.1.2 パスワード。**Tealium ネットワークの各ユーザーは、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 Single Sign On and Multifactor Authentication. Single sign on and Multifactor Authentication will be required for entry on all Tealium Network access points designed to restrict entry to authorized personnel.	**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、権限を有する人物以外の進入を制限するようデザインされたすべての Tealium のネットワークアクセスポイントで、進入する際に必要とされる。
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.	**10.2 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 Unsuccessful Logon Attempts. The number of unsuccessful logon attempts will be limited to a maximum of five (5). User accounts will be locked for at least ten (10) minutes after the maximum number of permitted unsuccessful logon attempts is exceeded.	**10.3 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 Remote Access. Remote access to Tealium Network containing Customer Data will be restricted to authorized users, will require Multifactor Authentication, and will be logged for review.	**10.4 遠隔アクセス。** 顧客データを収納する Tealium のネットワークの遠隔アクセスは、承認された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 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.	**10.5 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 Privileged Access. Tealium will use Industry Standard methods to provide that:	**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 users with access to Tealium Network containing Customer Data will be granted the minimum amount of privileges necessary to perform their jobs;	**10.6.1** 顧客データを収納する Tealium のネットワークにアクセスできるユーザーは、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 privileged access will be restricted to authorized	**10.6.2** 特権アクセスは、権限を付与された個人ユーザ

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 Network; and **10.6.5** all privileged access will require Multifactor Authentication.	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 のネットワーク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. 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 Network Processing Customer Data Tealium will: **11.2.1** maintain logs of key events, including access events, that may reasonably affect the confidentiality, integrity, and availability of the Services to Customer and that may assist in the identification or investigation of Security Incidents occurring on Tealium Network. Copies of such 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.	**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 のネットワークによる顧客データの処理のため、Tealium は以下を行う。 **11.2.1** 顧客に提供される本サービスの秘密保持、完全性、および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 のネットワーク上で発生しているセキュリティーインシデントの特定または調査に役立ちうる重要なイベント（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。 **11.2.2** ログ記録を修正または削除から保護する、 **11.2.3** 定期的にログ記録を見直す、 **11.2.4** 業界基準の形式でログ記録を保存する、また **11.2.5** ログ記録を少なくとも 12 ヶ月間保管する。
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 SDLC, which will be	**12 ソフトウェアセキュリティーに関する保証。** **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 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

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 Network failures or outages. Tealium will review capacity plans and performance monitoring information on a regular basis. **12.4 Software Security Testing Process**. Tealium will in the course of providing Services: **12.4.1** provide that applications undergo a formal code review process. Upon Customer's written request, Tealium will provide evidence of this formal process to Customer; **12.4.2** provide that applications undergo Dynamic Application Security Test (DAST), Source 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 **12.4.3** provide that applications undergo a Threat Model analysis at least annually. 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.	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、セキュリティー要件の定義付け、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 のネットワーク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。 **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。 **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。 **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)、ソースコード構成分析（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 **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。 **13 データセンターの管理。**

13. Data Center Controls. **13.1 Base Requirements**. Any data center supporting the Services will possess the following minimum requirements: **13.1.1** Adequate physical security and access controls as set forth in Sections 6 and 7 of this DSS; **13.1.2** Industry Standard HVAC & environmental controls; **13.1.3** Industry Standard network/cabling environment; **13.1.4** Industry Standard redundant and high capacity networking bandwidth; **13.1.5** Industry Standard fire detection/suppression capability; **13.1.6** Industry Standard uninterruptible power distribution; and **13.1.7** A comprehensive business continuity plan. **14. Business Continuity Plan (BCP).** **14.1 BCP Planning and Testing** **14.1.1** Tealium's plan capabilities will include data resiliency processes covering all hardware, software, communications equipment, and current copies of data and files necessary to perform Tealium's obligations under the MSA; and **14.1.2** Tealium will maintain processes for timely recovery of Services. **14.2 BCP Plan**. The plan will address the following additional standards or equivalent in all material respects: **14.2.1** The plan will reflect regulatory requirements and Industry Standards; **14.2.2** The relocation of affected Tealium personnel to one or more alternate sites, including remote work, and the reallocation of work to other locations that perform similar functions until such relocation is effected; **14.2.3** A full 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;	**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。： **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 **13.1.2** 業界基準の HVAC および環境管理 **13.1.3** 業界基準のネットワーク/ケーブルの環境 **13.1.4** 業界基準の冗長かつ大容量のネットワーク帯域 **13.1.5** 専門的火災探知/消化機能 **13.1.6** 業界基準の無停電電源の供給　および **13.1.7** 包括的事業継続プラン **14　事業継続プラン(BCP)。** **14.1 BCP プランおよびテスト** **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。 **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。 **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。： **14.2.1** 当プランは、規制および業界慣行を反映する。 **14.2.2** 影響を受ける Tealium のスタッフの代替地への移転（単独または複数回）（遠隔勤務を含む）、および当該移動が有効になるまでの間、同様の機能を果たすその他の場所への職務の移転。 **14.2.3** 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包括的業務影響度の分析。

14.2.4 The establishment and maintenance of alternate sites and systems, the capacity of which will be no less than the primary sites and systems that Tealium uses to provide the Services and perform its other obligations under the MSA;	**14.2.4** 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。
14.2.5 A description of the recovery process to be implemented following the occurrence of a disaster. The description will detail the contingency arrangements in place to ensure recovery of Tealium's operations, systems and processes and the key personnel, resources, services and actions necessary to ensure that business continuity is maintained; and	**14.2.5** 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。
14.2.6 A schedule of the objective times by which Tealium's operations, systems and processes will be recovered following the occurrence of a disaster. Tealium agrees that its recovery processes and BCP plans provide a Recovery Time Objective (RTO) of four (4) hours and a Recovery Point Objective (RPO) of 24 hours.	**14.2.6** 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。
14.3 Notification. In case of a disaster that Tealium reasonably believes will impact its ability to perform its obligations or affect the Services under the MSA, Tealium will promptly notify Customer of such disaster. Such notification will, as soon as such details are known, describe:	**14.3 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。
14.3.1 The disaster in question and how it was detected;	**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
14.3.2 The impact the disaster is likely to have on the Services;	**14.3.2** 大事故が本サービスに及ぼすと予想される影響
14.3.3 The alternative operating strategies and the back-up systems Tealium will utilize and the timetable for their utilization; and	**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
14.3.4 The expected timeframe in which the disaster will be resolved and Tealium expects to return to business as usual.	**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
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.	**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処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。

TEALIUM INC. DATA PROCESSING ADDENDUM No Standard Contractual Clauses (Addendum DPA-2)	TEALIUM INC. データ処理補足条項 非標準的契約条項 (補足条項 DPA-2)
This Data Processing Addendum ("DPA") forms part of, and is subject to, the Master Services Agreement or other written or electronic terms of service or subscription agreement between Tealium and Customer for Customer's purchase of Services from Tealium that references this DPA (the "MSA"). This DPA applies where there is no transfer of Personal Data between the European Union and the USA, or the UK and the USA.	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、その対象となる。本 DPA は、欧州連合と米国間、または英国と米国感に個人データの移動がない場合に適用される。
1. Definitions. For the purposes of this DPA, the terminology and definitions as used by Data Protection Laws and Regulations (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:	**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 にベット定義されない限り、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" means the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020).	**「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。
"Data Exporter" and **"Data Importer"** have the meanings given them in the Standard Contractual Clauses.	**「データエクスポータ」** および **「データインポータ」**は標準契約条項で与えられた意味を持つ。
"Data Protection Laws and Regulations" means all laws and regulations applicable to each respective Party in its role in the Processing of Personal Data under the MSA, including where applicable, the GDPR, the Privacy Act, the APPI, and US Privacy Laws.	**「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役割にに関して各当事者に適用されるすべての法律および規制をいい、 GDPR、プライバシー法、また CCPA が含まれる場合がある。
"Data Security Statement" or **"DSS"** means Tealium's statement of its technical and organizational security measures.	**「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" means, for the purpose of this DPA, the European Economic Area.	**「EEA」** とは、本 DPA の目的上、欧州経済領域および英国をいう。
"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.	**「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。
"Highly Sensitive Data" means personal data whose unauthorized disclosure or use could	**「極秘データ」**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

reasonably entail a serious potential security or privacy risk for a data subject, including but not limited to government issued identification numbers such as national insurance numbers, passport numbers, driver's license numbers, or similar identifier, or credit or debit card numbers, medical or financial information, biometric data, and/or financial, medical or other account authentication data, such as passwords or PINs.	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。
"Personal Data" has the meaning set forth in Data Protection Laws and Regulations relating to the collection, use, storage or disclosure of information about an identifiable individual, or if no definition, means information about an individual that can be used to identify, contact or locate a specific individual, or can be combined with other information that is linked to a specific individual to identify, contact or locate a specific individual. For purposes of the DPA, Personal Data is as described in the scope of Processing described in Appendix 1.	**「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、連絡し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、連絡し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 1 に記載のある「処理」の範囲に示される通りである。
"Privacy Act" means the Australian Privacy Act 1988 (Cth.).	**「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。
"Processing" or **"Process"** means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	**「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、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。
"Service Provider" shall have the meaning set forth in the CCPA.	**「サービスプロバイダー」**は、 CCPA に定義される意味を持つものとする。
"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data, but does not include any Unsuccessful Security Incident.	**「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をいう。ただし未然のセキュリティー事故を除く。
"Tealium Network" means the data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within the control of Tealium or its sub-processors and are used to provide the Services.	**「Tealium のネットワーク」**とは、Tealium またはそのサブプロセッサーの管理内にあり、かつ本サービスを提供するために使用される、データセンター施設、ネットワーク環境、およびホストソフ

"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.	トウェア（仮想ファイアーウォールなど）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。
"US Privacy Laws" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq (the ("CCPA"), the Virginia Consumer Data Privacy Act ("VCDPA"), the Colorado Privacy Act, and any similar state privacy law or regulation.	**"US Privacy Laws"「米国のプライバシー法」**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」）、ヴァージニア州消費者データプライバシー法（「VCDPA」）、コロラド州プライバシー法、および同様の州立プライバシー法または規制のすべてをいう。
"User Data" means the login details and contact information of the authorized users of the Services and will be deemed Personal Data.	**「ユーザーデータ」**とは、本サービスの使用を認められたユーザーのログイン情報の詳細および連絡先をいい、個人データとみなされる。
Further definitions are provided throughout this DPA.	より詳しい定義は本 DPA を通じて示される。
Data Processing.	**データ処理。**
2.1 Scope and Roles. This DPA applies where and only to the extent that Tealium Processes Personal Data on behalf of Customer as a data processor or Service Provider in the course of providing Services pursuant to the MSA. Tealium will engage sub-processors pursuant to the requirements for subcontractors set forth in Section 10 below.	**2.1 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ー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 は、以下セクション 10 で定められる下請業者の要件に従って、下請業者を雇用する。
2.2 Compliance with Laws. Each party will comply with all Data Protection Laws and Regulations applicable to it and binding on it in the provision or receipt of Services under the MSA, including all statutory requirements relating to data protection.	**2.2 法への準拠。** 各当事者は、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。
2.3 Customer Processing of Personal Data. Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which it acquired Personal Data. Customer will not transmit to Tealium nor require	**2.3 顧客による個人データの処理。** 顧客は、個人データの正確性、質、および合法性について、また顧客が個人データを得た方法について、単独で責任を負わなければならない。顧客は、Tealium に極秘データを送信せず、また Tealium にその処

Tealium to process any Highly Sensitive Data. As the owner and controller of the Personal Data, the statutory duties may include the following: (i) complying with Personal Data security and other obligations prescribed by Data Protection Laws and Regulations; (ii) establishing a procedure for the exercise of the rights of the individuals whose Personal Data is collected; (iii) only processing Personal Data that have been lawfully and validly collected and ensuring that such Personal Data is relevant and proportionate to the respective uses; (iv) ensuring that after assessment of the requirements of Data Protection Laws and Regulations, the security and confidentiality measures implemented are suitable for protection of Personal Data against any accidental or unlawful destruction, accidental loss, alteration, unauthorized or unlawful disclosure or access, in particular when the processing involves data transmission over a network, and against any other forms of unlawful or unauthorized processing; and (v) taking reasonable steps to ensure compliance with the provisions of this DPA by any person accessing or using Personal Data.

2.4 Instructions for Data Processing.

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

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

理を要求しない。個人データの所有者および監督者としての法定義務は以下を含む。(i)個人データ保護およびデータ保護法および規制に示されるその他の義務に遵守すること、(ii) 個人データを収集された個人の権利を行使するための措置を確立すること、(iii)適法かつ有効に収集された個人データのみを処理し、かかる個人データがそれぞれの利用に関連がありまた相当量であることを保証すること、(iv)データ保護法の要件を審査したのち、設置されたデータ保護および機密情報保持の措置が、データの偶発的または違法な破壊、偶発的な損失、変更、無許可のまたは違法な開示あるいはアクセス（特にデータ処理がネットワークを介してデータ送信が行われる場合）、およびその他あらゆる形態の違法または無許可のデータ処理に対する、個人データの保護に適していることを保証すること、および(v)個人データにアクセスまたは使用するすべての者によって、当 DPA の条項の遵守を保証するため合理的な措置を講じること。

2.4 データ処理の指示。

2.4.1 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、顧客にかか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しない。

2.4.2 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。

fees Customer will pay to Tealium for carrying out such instructions. **2.4.3** Customer shall ensure its processing instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws and Regulations or cause Tealium to be in breach of Data Protection Laws and Regulations. Tealium shall immediately inform Customer if, in its opinion, an instruction infringes any provision of Data Protection Laws and Regulations. In such case, Tealium is not obliged to follow the instruction unless and until Customer has confirmed or changed such instruction. **2.5 Disclosure.** Tealium will not disclose Personal Data to any third party other than as expressly permitted by the terms of the MSA, and except as necessary to comply with applicable laws and regulations or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Tealium a demand for Personal Data, Tealium will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Tealium may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then Tealium will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Tealium is legally prohibited from doing so. 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. **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.	**2.4.3** 顧客は、顧客の処理に関する指示が合法であること、個人データの処理が適用されるデータ保護法および規制に違反しないこと、あるいは Tealium がデータ保護法および規制に違反する事態を招かないことを確実にしなければならない。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。 **2.5 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。 **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

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

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

4. Other obligations of Tealium. Tealium will:

4.1 take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk. Such measures shall, at a minimum, meet the specifications set forth in the Data Security Statement;

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

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

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

Customer Controls and Data Subject rights.

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

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。

4. Tealium のその他の義務。 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的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 サブプロセッサーの雇用において本 DPA セクション 10 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。

顧客の制御権およびデータ主体の権利。

5.1 顧客の制御権。 本サービスは、顧客が、個人データを収得し、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。顧客は、以下の適切な実行に責任を負う。(a)本サービスのコンフィギュレーション、(b) 本サービスに関連して可能な制御権（セキュリティーコントロールを含む）の使用、(c) 個人データの適切なセキュリティー、保護、およびバックアップのために、顧客が適切であると判断した措置（不正アクセスから

backup of Personal Data, which may include use of encryption technology to protect Personal Data from unauthorized access, and routine archiving of Personal Data.

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

Transfers of Personal Data.

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

Security Responsibilities of Tealium.

7.1 Continued Evaluation. In addition to its obligations under Section 4.1 of this DPA, Tealium will conduct periodic reviews of the security of its infrastructure, applications, and associated Services. The adequacy of Tealium's information security program is measured against industry security standards and compliance with Tealium's policies and procedures. Tealium will continually evaluate the security of the Tealium Network and associated Services to determine whether additional or mitigating security measures are required to respond to new security risks or findings generated by the periodic reviews. Tealium

個人データを保護するための暗号化技術の使用、および個人データの定期的アーカイブも含まれうる）の実行。

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。

個人データの転送。

リージョン。 顧客は、以下のリストに挙げられる Tealium のネットワーク内の、個人データ（ユーザーデータを除く）がホストされる場所を選ぶことができる（かかるリストは Tealium によって随時更新される）。(i) 米国、(ii) アイルランド、(iii) ドイツ、(iv)日本、(v)　オーストラリア、および(vi)香港 (それぞれ「リージョン」という)。顧客が本サービスを適切に設定して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。

Tealium のセキュリティー責任。

7.1 継続的評価。 本 DPA セクション 4.1 に基づく義務に加え、Tealium は、自身のインフラストラクチャ、アプリケーション、および関連する本サービスのセキュリティーを定期的に評価する。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

conducts ongoing vulnerability scans and annual penetration tests to identify and then remediate identified deficiencies. The Tealium Network and associated Services are continuously monitored for events and potential Security Incidents. Tealium also conducts risk assessments at least annually or when significant changes to the environment occur. These activities provide for a continually improving information security program.	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。
7.2 Customer Independent Review. Customer acknowledges that it is responsible for reviewing the information made available by Tealium relating to data security and making an independent determination as to whether the Services meet Customer's requirements. Customer is responsible for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.	**7.2 顧客の独自の審査。** 顧客は、 データセキュリティーに関して Tealium に開示された情報を審査し、また本サービスが顧客の要求を満たすかどうかを独自に判断する責任があることを認める。顧客は、顧客の人員と相談役がデータセキュリティーに関して提供されたガイドラインに従うことを保証する責任がある。
Certifications and Audits.	**サティフィケーションおよび監査。**
8.1 Tealium Audits. Tealium audits its privacy and security measures at least annually. These audits will be performed according to ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27018 and SOC 2 Type II standards or such other alternative standards that are substantially equivalent to such standards. These audits will be performed by independent third party security professionals at Tealium's selection and expense.	**8.1 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、ISO/IEC 27701、 ISO/IEC 27018 、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。
8.2 Audit Reports. At Customer's written request, Tealium will provide Customer with either a certificate or a confidential report so that Customer can reasonably verify Tealium's compliance with its obligations under this DPA. The report constitutes Tealium's Confidential Information.	**8.2 監査の報告。** 顧客の要請を受けた場合、顧客が、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 は、顧客に機密報告書を提出する。かかる報告書は Tealium の本秘密情報を構成する。
8.3 Customer Audits. Customer audits rights are as set forth in the DSS.	**8.3 顧客の監査。**顧客の監査に関する権利は、DSS に定義される。
9. Security Incident Notification.	**9. セキュリティーインシデントの通知。**

9.1 Tealium Notification. If Tealium becomes aware of a Security Incident, Tealium will without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify Customer of the Security Incident. Where the notification to the Customer is not made within 48 hours, it shall be accompanied by reasons for the delay.	**9.1 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。
9.2 The notification referred to in Section 9.1 shall at least:	**9.2** セクション 9.1 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。:
9.2.1 describe the nature of the Security Incident;	**9.2.1** セキュリティーインシデントの性質の説明
9.2.2 communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;	**9.2.2** 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
9.2.3 describe the measures taken or proposed to be taken by Tealium to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects.	**9.2.3** 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。
9.3 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.	**9.3** 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。
9.4 Tealium shall document any Security Incidents, comprising the facts relating to the Security Incident, its effects and the remedial action taken.	**9.4** 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。
9.5 Tealium Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under the Data Protection Laws and Regulations, Tealium will include in the notification under section 9.1 such information about the Security Incident as Tealium is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Tealium, and any restrictions on disclosing the information, such as confidentiality.	**9.5 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 9.1 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。
9.6 Unsuccessful Security Incidents. Customer agrees that:	**9.6 制限。**顧客は以下の点に合意する。:
9.6.1 An Unsuccessful Security Incident will not be subject to this Section; and	**9.6.1** 未然のセキュリティーインシデントは当セクションの対象にならないこと。
9.6.2 Tealium's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by	**9.6.2** 当セクションに基づく Tealium のセキュリティーインシデントの報告または応対は、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

Tealium of any fault or liability of Tealium with respect to the Security Incident.

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

10. Sub-Processing.

10.1 Authorized Sub-processors. Customer agrees that Tealium may use the sub-processors set forth at Tealium Sub-Processors Page to fulfill certain of its contractual obligations under this DPA or to provide certain services on 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. Notice may include an update to the applicable website and providing Customer with a mechanism to obtain notice of that update.

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

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

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

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

10.3 Objection to Sub-Processor. If Customer has a reasonable basis to object to Tealium's use of a new sub-processor, Customer shall notify Tealium promptly in writing within ten (10) business days after receipt of Tealium's notice. If Customer

にはならず、将来的にもそうならないこと。

9.7 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。

10. サブプロセス。

10.1 権限を付与されたサブプロセッサー。 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 がサブプロセッサーとして AWS を利用できることに同意する。Tealium は、サブプロセッサーの追加または変更を意図する場合、顧客がその変更に異議を申し立てることができるよう、顧客にその意図を通知する。 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。

10.2 サブプロセッサーに関する義務。 当セクション 10 に示される通り、Tealium がサブプロセッサーに権限を与える場合、Tealium は以下を実行する。:

10.2.1 Tealium は、サブプロセッサー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、サブプロセッサー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。

10.2.2 Tealium は、サブプロセッサーに 、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ーおよび監査の権利を含む関連した契約義務を含む。

10.2.3 Tealium は、本 DPA の義務の Tealium の履行、およびサブプロセッサー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。

10.3 サブプロセッサーへの異議。 顧客が、Tealium による新しいサブプロセッサーの採用に

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

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

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

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

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 10 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ーに反対する場合、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ー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ーの使用なしに 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。

11. 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。

12. DPA の解約。本 DPA は、 MSA の解約日（「本解約日」）まで 有効である。

13. 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、個人データの収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。本解約日まで、顧客は、当セクションに従って個人データ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 日以内に個人データ

termination or expiration of the MSA, Tealium will delete Personal Data within 90 days following the Termination Date. In any event, Tealium will delete Personal Data within 180 days following the Termination Date. **14. Fees and Expenses.** To the extent legally permitted, Customer shall be responsible for any costs and fees arising from a request by Customer to change the Region originally chosen by Customer during configuration of its account(s) pursuant to Section 6 above. **15. Nondisclosure.** Customer agrees that the details of this DPA are not publicly known and constitute Tealium's Confidential Information under the confidentiality provisions of the MSA. **16. Conflict.** Except as amended by this DPA, the MSA will remain in full force and effect. If there is a conflict between the MSA and this DPA, the terms of this DPA will control.	を消去する。いかなる場合であっても、Tealium は、本解約日から 180 日以内に個人データを消去する。 **14. 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。 **15. 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。 **16. 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。