PSLT – Real-time Customer Data Platform (2020v1)

1. **Customer Responsibilities.** Customer is solely responsible for:
   1.1 ensuring that all data ingested into Real-time Customer Data Platform adheres to XDM standards;
   1.2 ensuring that all data ingested into Real-time Customer Data Platform has been assigned the appropriate DULE label(s);
   1.3 ensuring that appropriate data use policies (e.g., based on Customer's privacy notices, contractual rights, and consent-based rights) have been implemented, and are executed, within Real-time Customer Data Platform; and
   1.4 ensuring that the Privacy Service API is only used to process data access, correction and deletion requests originated by individual data subjects.

   Adobe will not be responsible for any failure in the operation of Real-time Customer Data Platform caused by Customer's failure to meet the obligations outlined in sections 1.1 to 1.3 above.
2. **Data Retention**
   2.1 **Profile Service.** Behavioral/time series data appended to any Profile may be deleted from Real-time Customer Data Platform 30 days from the date of its addition to a Profile or until some alternative time period selected by Customer within Real-time Customer Data Platform.
   2.2 **Data Lake.** Customer Data stored in the Data Lake will be retained:
      (A) for 7 days to facilitate the onboarding of Customer Data into the Profile Services, after which it may be permanently deleted;
      (B) for 180 days to facilitate any use case involving Customer AI Intelligent Service training or processing, after which it may be permanently deleted; or
      (C) until deleted by Customer.
3. **Transmitted Data.** Upon request by Customer, Adobe will send specified Transmitted Data to a Targeting Platform on behalf of Customer. Customer is responsible for ensuring that any use or combination of the Transmitted Data (by Customer, the Targeting Platform, or other third parties) complies with all applicable laws, guidelines, regulations, codes, rules, and established industry best practices for data usage and privacy (such as the DAA Self-Regulatory Principles when applicable).
4. **Use of a Targeting Platform.** Adobe's transfer of Transmitted Data to a Targeting Platform does not grant to Targeting Platform, or other third parties, the right to (i) access Adobe's online reporting interface or tools, or (ii) receive Reports. Adobe does not control, or have responsibility for, either the use of the Transmitted Data by Customer through the Targeting Platform or for Customer's combination of the Transmitted Data with any other data through the Targeting Platform's technology or services. Customers using People-based Destinations must (a) provide Adobe with hashed identifiers and (b) obtain any necessary permissions from its site visitors (as may be required by law or industry guidelines).
5. **Ad Targeting.** If Customer is either located in the U.S. or uses the On-demand Services on Customer Sites directed towards visitors located in the U.S., Customer must abide by the DAA Self-Regulatory Principles in connection with its use of the On-demand Services, as applicable.
6. **Prohibited Data.** Customer must ensure that neither Customer nor any Targeting Platform combines or otherwise links Prohibited Data with Protected Data or takes any other action that would convert Protected Data to Prohibited Data. Customer must properly label Protected Data within the On-demand Services and ensure that policies are established and executed to prevent the combination or linking of Protected Data and Prohibited Data.
7. **Additional Claims**. Customer's indemnification obligations set forth in the General Terms will also apply to third-party Claims that relate to or arise from the use, display, exchange, or transfer of Transmitted Data between

and among Targeting Platforms, Customer and Adobe. The additional Claims in this section are treated as Data Privacy Claims or Other Claims as described in the applicable General Terms. The Limitation of Liability provision in the applicable General Terms does not apply to third-party Claims brought against Adobe by social media Targeting Platforms (e.g., Facebook, Google, Twitter or Amazon) that arise from Customer's use of Real-time Customer Data Platform.

8. **Definitions.**

8.1 "**DAA**" means Digital Advertising Alliance.

8.2 "**Directly Identifiable Information**" means information that can be used to directly identify an individual person, including Stable Identifiers.

8.3 "**Directly Identifiable Profile**" means a merged Profile that includes Directly Identifiable Information.

8.4 "**DULE**" means Adobe's Data Usage, Labeling and Enforcement governance framework.

8.5 "**People-based Destinations**" means people-based Targeting Platforms (e.g., social networks) that require the use of hashed identifiers.

8.6 "**Profile**" means a record of information representing an individual (including Directly Identifiable Profiles and Pseudonymous Profiles) as represented in the Profile Service.

8.7 "**Prohibited Data**" means data which would allow Adobe to directly identify a specific natural person (rather than their device), such as their telephone number, email address, government issued identification number, name, postal address.

8.8 "**Protected Data**" means any pseudonymous profile data:

(A) intended to be used for Online Behavioral Advertising (as defined by the DAA); or

(B) that Customer (or its third-party data providers) have otherwise identified as data that cannot be combined with Prohibited Data.

8.9 "**Pseudonymous Profile**" means a merged Profile that includes no Directly Identifiable Information.

8.10 "**Stable Identifier**" means any identifier other than a cookie ID or device ID.

8.11 "**Targeting Platform**" means any entity (e.g., demand-side platform, ad server, or content management platform) that has:

(A) entered into:

(1) an agreement with Customer authorizing such entity to access and use Transmitted Data; or

(2) a data access agreement with Adobe to access and use Transmitted Data sent on behalf of, and as directed by Customer; and

(B) an active integration with Adobe for use with Real-time Customer Data Platform.

Customer acknowledges and agrees that Adobe does not and cannot guarantee the availability of specific Targeting Platforms.

8.12 "**Transmitted Data**" means Customer Data imported into, or exported from, the On-demand Service.

8.13 "**XDM**" means the Experience Data Model documented at https://**github**.com/adobe/xdm.

PSLT – Real-time Customer Data Platform (2020v1)

1. **お客様の責任。**お客様は以下に関して全責任を負うものとします。
   1.1 Real-time Customer Data Platformに取り込まれたすべてのデータがXDM標準に準拠していることの保証。
   1.2 Real-time Customer Data Platformに取り込まれたすべてのデータに対して適切なDULEラベルが割り当てられることの保証。
   1.3 （お客様のプライバシー通知、契約上の権利、および同意に基づく権利などに基づく）適切なデータ使用ポリシーがReal-time Customer Data Platformで実施および履行されていることの保証。
   1.4 Privacy Service APIが、個々のデータ主体から生じたデータアクセス、修正、削除要求のみを処理するために使用されることの保証。

   アドビは、上記第1.1項および第1.3項までに定められたお客様の義務の不履行に起因するReal-time Customer Data Platformの運用におけるいかなる障害に関しても責任を負いません。
2. **データの保存**
   2.1 **プロファイルサービス。**プロファイルに加えられた行動/時系列データは、プロファイルに追加された日から30日後、またはReal-time Customer Data Platform内でお客様が選択した別の期間にReal-time Customer Data Platformから削除されることがあります。
   2.2 **データレイク。**データレイクに保存されたお客様データは次の期間保持されます。
      (A) プロファイルサービスへのお客様データのオンボーディングを促進するために、7日間。その後、永久に削除することができます。
      (B) お客様 AI Intelligent Serviceのトレーニングまたは処理に関連するユースケースを推進するために、180日間。その後、永久に削除することができます。
      (C) お客様が削除するまで。
3. **送信されたデータ。**お客様から要請があった場合、アドビはお客様の代理として、特定の送信されたデータをターゲティングプラットフォームに送信します。お客様は、送信されたデータのあらゆる使用または組み合わせ（お客様、ターゲティングプラットフォーム、もしくはその他の第三者によるものを含めて）が、適用されるすべての法令、ガイドライン、規制、規範、規則、および確立された業界のベストプラクティス（該当する場合、DAA自主規制原則など）を遵守していることを保証する責任を負います。
4. **ターゲティングプラットフォームの使用。**アドビが送信されたデータをターゲティングプラットフォームに転送する場合でも、それはターゲティングプラットフォームまたはその他の第三者に、(i) アドビのオンラインレポーティングインターフェイスもしくはツールにアクセスする権利、または (ii) レポートを受け取る権利を付与するものではありません。アドビは、お客様による、ターゲティングプラットフォームを介しての、送信されたデータの使用、またはターゲティングプラットフォームのテクノロジーもしくはサービスを用いての送信されたデータと他のいかなるデータとの組み合わせについても、それらを管理せず、それらに対する責任も負いません。ピープルベースの配信先を使用するお客様は、(a) ハッシュ化された識別子をアドビに提供する、および (b) サイト訪問者から（法律または業界ガイドラインの規定に従い）必要な許可を取得する必要があります。
5. **広告のターゲティング。**お客様が米国内に所在する場合、または米国内に所在するサイト訪問者向けのお客様サイトでオンデマンドサービスを利用する場合、お客様はオンデマンドサービスの利用に関連して、該当するDAA自主規制原則に従わなければなりません。

6. **禁止データ。**お客様は、お客様もターゲティングプラットフォームも、禁止データと保護されたデータを組み合わせたり、どのような方法であれそれらを結び付けたり、保護されたデータを禁止データに変換することになるその他の措置を講じたりしないようにする必要があります。お客様は、オンデマンドサービス内の保護されたデータを適切に分類し、保護されたデータと禁止データの組み合わせや結び付けを防ぐためのポリシーを策定し、実行する必要があります。

7. **追加の申立て等。**アドビ基本利用条件に定めるお客様の補償義務は、ターゲティングプラットフォーム、お客様およびアドビ間での送信されたデータの使用、表示、交換、もしくは転送に関連または起因する第三者の申立て等にも適用されます。本項の追加の申立て等は、適用されるアドビ基本利用条件に記載される、データプライバシー関連申立て、またはその他の申立て等として扱われます。適用されるアドビ基本利用条件の責任の制限規定は、お客様がReal-time Customer Data Platformを使用することから生じる、ソーシャルメディアターゲティングプラットフォーム（Facebook、Google、Twitter、Amazonなど）によるアドビに対する第三者の申立て等には適用されません。

8. **定義。**

8.1 「**DAA**」はDigital Advertising Allianceの略称です。

8.2 「直接識別可能情報」とは、直接的に個人を特定するために使用できる情報（安定識別子を含む）を指します。

8.3 「直接識別可能プロファイル」とは、統合されたプロファイルで直接識別可能情報を含むものを指します。

8.4 「**DULE**」とは、アドビによるデータ使用、ラベリングおよび実施に関するガバナンスのフレームワークを指します。

8.5 「**ピープルベースの配信先**」とは、ハッシュ化された識別子の使用が義務付けられる、人を対象とするターゲティングプラットフォーム（ソーシャルネットワークなど）を意味します。

8.6 「**プロファイル**」とは、プロファイルサービスに表示されている個人を表す情報の記録（直接識別可能プロファイルおよび匿名プロファイルを含みます）を意味します。

8.7 「**禁止データ**」とは、アドビが特定の自然人（かかる人物のデバイスではなく）を直接に識別することができるデータ（かかる人物の電話番号、メールアドレス、政府発行のID番号、氏名、郵便番号等）を意味します。

8.8 「**保護されたデータ**」とは、以下の匿名のプロファイルデータを意味します。

(A) オンライン行動ターゲティング広告（DAAの定義による）のための使用を目的とするデータ、または

(B) お客様（またはお客様の第三者データプロバイダー）が禁止データと組み合わせることができないデータとして特定しているデータ。

8.9 「**匿名プロファイル**」とは、統合されたプロファイル（直接識別可能情報を除きます）を指します。

8.10 「**安定識別子**」とは、Cookie IDもしくはデバイスID以外のすべての識別子を指します。

8.11 「**ターゲティングプラットフォーム**」とは、以下を有する事業体（デマンドサイドプラットフォーム、広告サーバー、またはコンテンツ管理プラットフォームなど）を意味します。

(A) 契約締結：

(1) かかる事業体に送信されたデータへのアクセスおよびその使用を許可するという、お客様との契約、または

(2) お客様の代理として、およびお客様の指示により送られた送信されたデータにアク

セスして利用するための、アドビとのデータアクセス契約、および

(B) Real-time Customer Data Platformと共に使用するためのアドビとのアクティブな統合。

お客様は、アドビが特定のターゲティングプラットフォームの可用性を保証できないことを了承し、これに同意するものです。

8.12 「**送信されたデータ**」とは、オンデマンドサービスにインポートされた、またはオンデマンドサービスからエクスポートされたお客様データを意味します。

8.13 「**XDM**」とは、https://**github**.com/adobe/xdmで文書化されたエクスペリエンス データ モデルを指します。