PSLT – Adobe Experience Platform Activation (2020v1)

1. **Customer Responsibilities.** Customer is solely responsible for:

    1.1   all testing of Customer Customizations, including security testing;

    1.2   ensuring that all data ingested into Adobe Experience Platform Activation adheres to XDM standards;

    1.3   ensuring that all data ingested into Adobe Experience Platform Activation has been assigned the appropriate DULE label(s);

    1.4   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 Adobe Experience Platform Activation; and

    1.5   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 or security of Adobe Experience Platform caused by Customer Customizations or Customer's failure to meet the obligations outlined in sections 1.1 to 1.4 above.

2. **Data Retention**

    2.1   **Profile Service.** Behavioral/time series data appended to any Profile may be deleted from Adobe Experience Platform Activation 30 days from the date of its addition to a Profile or until some alternative time period selected by Customer within Adobe Experience Platform Activation.

    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 Adobe Experience Platform Activation.

8. **Definitions.**

8.1 "**Customer Customizations**" means the customizations made to Adobe Experience Platform Activation by Customer or at Customer's direction. Customer owns (or, where applicable, must ensure it has a valid license to) Customer Customizations, subject to Adobe's underlying intellectual property in the Adobe Technology.   Customer acknowledges and agrees that Adobe's access to Customer Customizations does not preclude Adobe from independently developing (without use of Customer Customizations) or acquiring similar technology without obligation to Customer.

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

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

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

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

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

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

8.8 "**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.

8.9 "**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.

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

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

8.12 "**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 Adobe Experience Platform Activation.

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

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

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