



PSLT – Adobe Audience Manager Expanded Activation (2024v1)

1. **Customer Responsibilities.** Customer is solely responsible for ensuring that all privacy (including data export) controls in Adobe Audience Manager have been implemented, and are executed, within Adobe Audience Manager. Customer is responsible for refreshing Customer Data within Adobe Experience Platform to reflect updates or changes to Customer Data in Adobe Audience Manager.
2. **Data Retention.** Customer Data in Adobe Audience Manager will be deleted in accordance with the data retention terms in Customer's Agreement for Adobe Audience Manager. Customer Data in Adobe Experience Platform may be deleted 14 days from the date it is imported by Customer from Adobe Audience Manager.
3. **Transmitted Data.** Customer may use Adobe Experience Platform to send specified Transmitted Data to People-based Destinations. Customer represents and warrants that any use, display, exchange, transfer, or combination of the Transmitted Data by Customer or People-based Destinations to which Transmitted Data is sent complies with all applicable laws, guidelines, regulations, codes, rules, and established industry best practices for data usage and privacy (such as the Digital Advertising Alliance (DAA) Self-Regulatory Principles or National Advertising Initiative (NAI) Code of Conduct, as applicable).
4. **Use of People-based Destinations.** The transfer of Transmitted Data to a People-based Destination does not grant to such People-based Destination 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 People-based Destination or for Customer's combination of the Transmitted Data with any other data through the People-based Destination's technology or services. Customer must (a) anonymize (e.g., through "hashing" or substantial redaction) any unique identifiers in the Transmitted Data to be sent to People-based Destinations and (b) obtain any necessary permissions from its site visitors (as may be required by law or applicable self-regulatory principles and industry guidelines). Customer acknowledges and agrees that Adobe does not and cannot guarantee the availability of specific People-based Destinations.
5. **Prohibited Data.** Customer must ensure that Customer and People-based Destinations to which Customer sends its data: (A) do not transmit, provide, or otherwise make available to Adobe any Prohibited Data, and (B) do not derive Prohibited Data by any linking of, combination, or cross-comparison of, the Transmitted Data with other data that Customer or the Targeting Platform may possess or acquire from third party sources.
6. **Definitions.**
 - 6.1 **"People-based Destinations"** means people-based Targeted Destinations (e.g., social networks) that require the use of hashed identifiers and are available through Adobe Experience Platform.
 - 6.2 **"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.
 - 6.3 **"Targeted Destinations"** means any entity (e.g., demand-side platform, ad server, or content management platform, or any other partner of Customer) 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.
 - 6.4 **"Transmitted Data"** means Customer Data imported into, or exported from, the On-demand Service.