Consent processing in Adobe Experience Platform

Adobe Experience Platform allows you to process the consent data you have collected from your customers and integrate it into your stored customer profiles. This consent data can then be used by a consent-management platform (CMP) or your own downstream processes to determine whether data collection occurs for a specific customer, or whether their profiles are included in exported audience segments.

This document provides an overview of how to configure your Platform data operations to ingest customer consent data generated by your CMP and integrate that data into customer profiles for downstream use cases.

> [!NOTE]
>
> This document focuses on processing consent data using the Adobe standard. If you are processing consent data in compliance with the IAB Transparency and Consent Framework (TCF) 2.0, see the guide on TCF 2.0 support in Real-time Customer Data Platform.

Prerequisites

This guide requires a working understanding of the various Experience Platform services involved in processing consent data:

- Experience Data Model (XDM): The standardized framework by which Experience Platform organizes customer experience data.
- Adobe Experience Platform Identity Service: Solves the fundamental challenge posed by the fragmentation of customer experience data by bridging identities across devices and systems.
- Real-time Customer Profile: Leverages [!DNL Identity Service] to create detailed customer profiles from your datasets in real-time. Real-time Customer Profile pulls data from the Data Lake and persists customer profiles in its own separate data store.
- Adobe Experience Platform Web SDK: A client-side JavaScript library that allows you to integrate various Platform services into your customer-facing website.
    - SDK consent commands: A use-case overview of the consent-related SDK commands shown in this guide.
- Adobe Experience Platform Segmentation Service: Allows you to divide Real-time Customer Profile data into groups of individuals that share similar traits and will respond similarly to marketing strategies.

Consent processing flow summary {#summary}

The following describes how consent data is processed after the system has been properly configured:

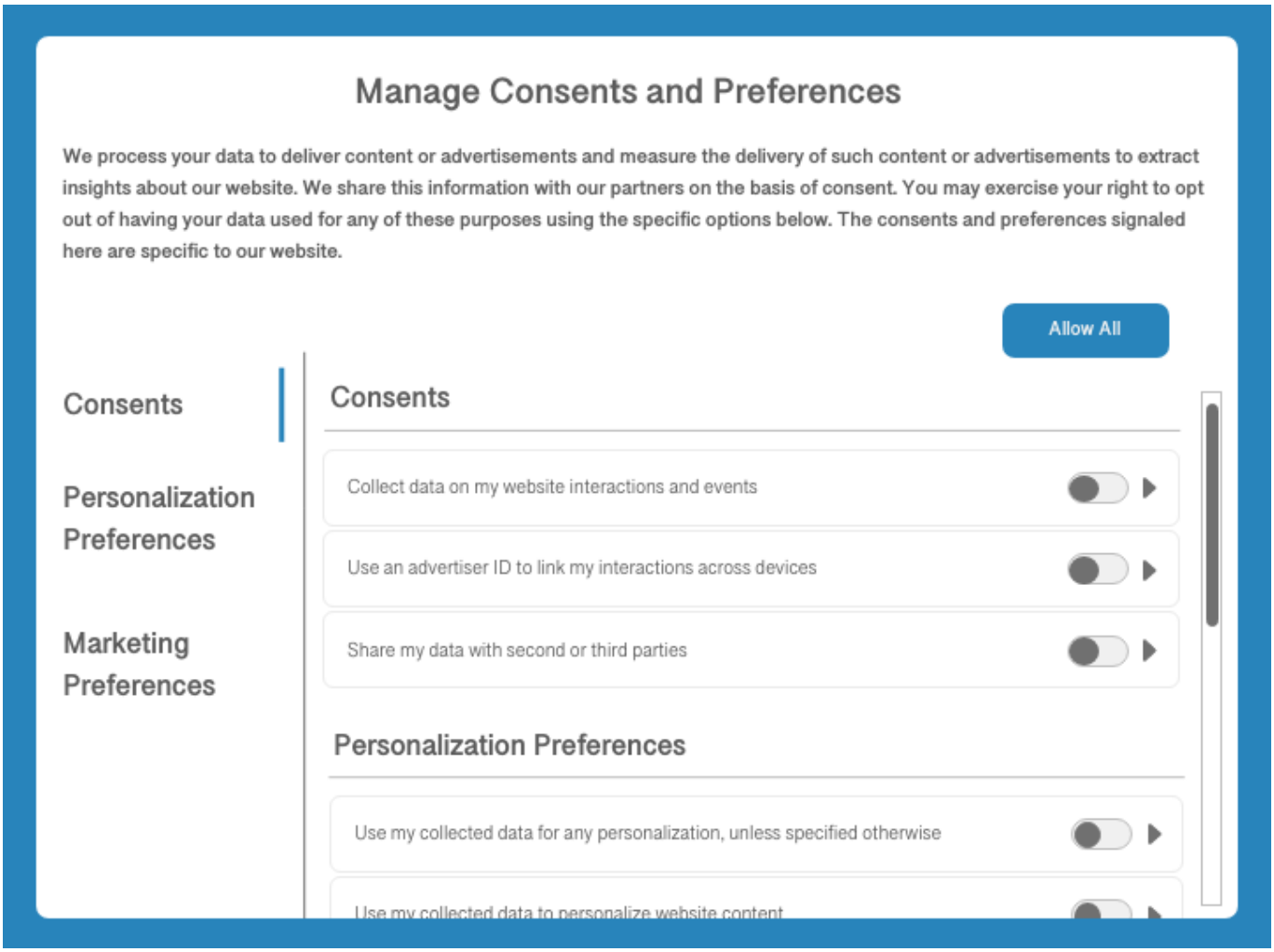
1. A customer provides their consent preferences for data collection through a dialog on your website.
2. On each page load (or when your CMP detects a change in consent preferences), a custom script on your site maps the current preferences to a standard XDM schema before passing it to the Platform Web SDK `setConsent` command.
3. When `setConsent` is called, the Platform Web SDK checks whether the consent values are different from those it last received. If the values are different (or there is no previous value), the structured consent/preference data is sent to Adobe Experience Platform.

4. The consent/preference data is ingested into a [!DNL Profile]-enabled dataset whose schema contains consent/preference fields.

In addition to SDK commands triggered by CMP consent-change hooks, consent data can also flow into Experience Platform through any customer-generated XDM data that is uploaded directly to a [!DNL Profile]-enabled dataset.

Determine how to generate customer consent data within your CMP {#consent-data}

Since each CMP system is unique, you must determine the best way to allow your customers to provide consent as they interact with your service. A common way to achieve this is through the use of a cookie consent dialog, similar to the following example:



This dialog should allow the customer to opt in or out of specific marketing and personalization use cases for their data. These consents and preferences should conform to the data model that you define for the [!DNL Profile]-enabled dataset in the next step.

Add standardized consent fields to a [!DNL Profile]-enabled dataset {#dataset}

Customer consent data must be sent to a [!DNL Profile]-enabled dataset whose schema contains consent fields. These fields should be included in the same schema and dataset that you use to capture attribute information about individual customers.

Refer to the tutorial on configuring a dataset for capturing consent data for detailed steps on how to add these required fields to a [!DNL Profile]-enabled dataset before continuing with this guide.

Update [!DNL Profile] merge policies to include consent data {#merge-policies}

Once you have created a [!DNL Profile]-enabled dataset for processing consent data, you must ensure that your merge policies have been configured to always include consent fields in each customer profile. This involves setting dataset precedence so that your consent dataset is prioritized over other potentially conflicting datasets.

For more information on how to work with merge policies, refer to the merge policies user guide. When setting up your merge policies, you must ensure that your profiles include all the required consent attributes provided by the Consents & Preferences mixin, as outlined in the guide on dataset preparation.

Bring consent data into Platform

Once you have your datasets and merge policies to represent the required consent fields in your customer profiles, the next step is to bring the consent data itself into Platform.

Primarily, you should be using the Adobe Experience Platform Web SDK to send consent data to Platform whenever consent-change events are detected by your CMP. If you already have consent data stored elsewhere, however, you can also opt to ingest your collected consent data directly by mapping it to your consent dataset's XDM schema and sending it to Platform through batch ingestion.

Details for each of these methods are provided in the subsections below.

Integrate the Experience Platform Web SDK to process customer consent data {#sdk}

Once you have configured your CMP to listen for consent-change events on your website, you can integrate the Experience Platform Web SDK to receive the updated consent settings and send them to Platform whenever a consent-change event occurs. Follow the guide on configuring the SDK to process customer consent data for more information.

Ingest XDM-compliant consent data directly {#batch}

You can ingest XDM-compliant consent data from a CSV file by using batch ingestion. This can be useful if you have a backlog of previously collected consent data that has yet to be integrated into your customer profiles.

Follow the tutorial on mapping a CSV file to XDM to learn how to convert your data fields to XDM and ingest them into Platform. When selecting the [!UICONTROL Destination] for the mapping, ensure that you select the **[!UICONTROL Use existing dataset]** option and choose the [!DNL Profile]-enabled consent dataset you created earlier.

Test your implementation {#test-implementation}

After you have ingested customer consent data into your [!DNL Profile]-enabled dataset, you can check your updated profiles to see whether they contain consent attributes.

> [!IMPORTANT]

> In order to view the attributes of an existing profile in the UI, you must know at least one identity value (and its corresponding namespace) associated with that profile.
>
> If you do not have access to this information, you can opt to ingest your own test consent data and associate it with an identity value/namespace that is known to you instead.

See the section on browsing profiles by identity in the [!DNL Profile] UI guide for specific steps on how to look up the details of a profile.

Note that the new consent attributes will not appear on a profile's dashboard by default, and therefore you must navigate to the **[!UICONTROL Attributes]** tab on the details page of a profile in order to confirm that they have been ingested as expected. See the guide on the profile dashboard to learn how to customize the dashboard to suit your needs.

Next steps

This guide covered how to configure your Platform operations to process customer consent data using the Adobe standard, and have those attributes represented in customer profiles. You can now integrate customer consent preferences as a determining factor in segment qualification and other downstream use cases.

For more information on Experience Platform's privacy-related capabilities, see the overview on governance, privacy, and security in Platform.