

IT Conversation Guide

If you're looking at implementing Adobe Audience Manager, it's helpful for marketing and IT to work together in the evaluation process. This conversation guide is designed to help foster a productive dialogue between your marketing and IT teams regarding key points you will need to consider. It provides basic answers to some of the initial questions IT will ask. The guide will also help you make joint decisions about deploying Adobe Audience Manager in a way that best fits both teams' needs.

"While marketers can play a key role in leading the CX charge, the ability to delight customers transcends the marketing function...A cross-team approach ultimately means ensuring that employees are motivated to work together across departments in order to bring about the best experience for customers."

—Econsultancy 2018 Digital Trends

Things IT will want to know.

How does Adobe Audience Manager handle Directly Identifiable Information?

Whether it's driven by GDPR (General Data Protection Regulation) or other privacy regulations and laws, your IT team will want to make sure Adobe Audience Manager has mechanisms in place to help ensure that your data collection efforts remain compliant. First of all, Audience Manager is configured to reject any Directly Identifiable Information (DII) from customers. If you try to import a file that contains email addresses, names, or other DII, the product has rules in place to help detect that type of content and block it from uploading when detected. That said, it is ultimately your responsibility to make sure you comply with your contractual obligations and only send Audience Manager data that contains pseudonymous identifiers.

Additionally, Audience Manager strictly employs pseudonymous ID synchronization methods when collecting web visitor data, and it only stores pseudonymous user ID mappings. These pseudonymous user ID mappings might include Audience Manager cookie IDs, Adobe Experience Cloud IDs, third-party cookie IDs, CRM IDs, and device advertising IDs.

How has Audience Manager been architected for scalability?

Your IT team will want to make sure Audience Manager has the

ability to process all of your permitted end-visitor data. Specifically, they will want insights on aspects of the Audience Manager storage and processing infrastructure that enable it to scale to meet your current and future loads. It's helpful to understand that Audience Manager already has a track record of handling the upload of millions of records on a regular basis. Some customers process almost 1TB of data with the product on a nightly basis. Adobe has designed the Audience Manager systems and infrastructure to support monthly data growth rates that have increased about 25% on average over the past two years. During peak times, Audience Manager regularly handles 4 million requests a minute and typically operates with excess capacity of 3-10X at its regional data stores.

All components of Audience Manager are hosted on Amazon Web Services (AWS), which includes Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3) in the United States, European Union, and Asia Pacific. Additionally, Audience Manager uses AWS Elastic Load Balancing to load balance requests within a given cluster.

How much effort is required to implement data collection in Audience Manager?

Implementing Audience Manager is fairly straightforward and doesn't require much customization. It comes with a JavaScript library that

enables live data collection of activity on your website, declared ID targeting to allow the exchange and synchronization of user IDs from devices and browsers that don't accept third-party cookies, and third-party pixel synchronization for retargeting purposes.

You can deploy the Audience Manager library directly onto your web pages—or, to simplify deployment, you can use a tag management solution of your choice. If you use Adobe Cloud Platform Launch, you can further simplify deployment by leveraging its automated tag management features specific to Audience Manager. Adobe Cloud Platform Launch is included with all Adobe Experience Cloud solutions.

Do Audience Manager requests impact web page performance?

Adobe designed Audience Manager to minimize potential impact on the performance of your environment. As a result, Audience Manager has tested at an average latency of 5 milliseconds from the edge of our data centers. Additionally, to keep any potential slow responses from impacting your page availability, read requests to Audience Manager Data Collection Servers will time out after 20 milliseconds. On average, Audience Manager handles 175,000 queries per second, but it has peaked at over 300,000 queries per second.

Furthermore, to optimize performance of third-party pixel synchronization used in retargeting, Audience Manager loads ID synchs asynchronously in an IFRAME. These occur at the bottom of the page load, so they don't slow down Audience Manager calls—and so that ID synchs don't delay the passing of IDs into the product.

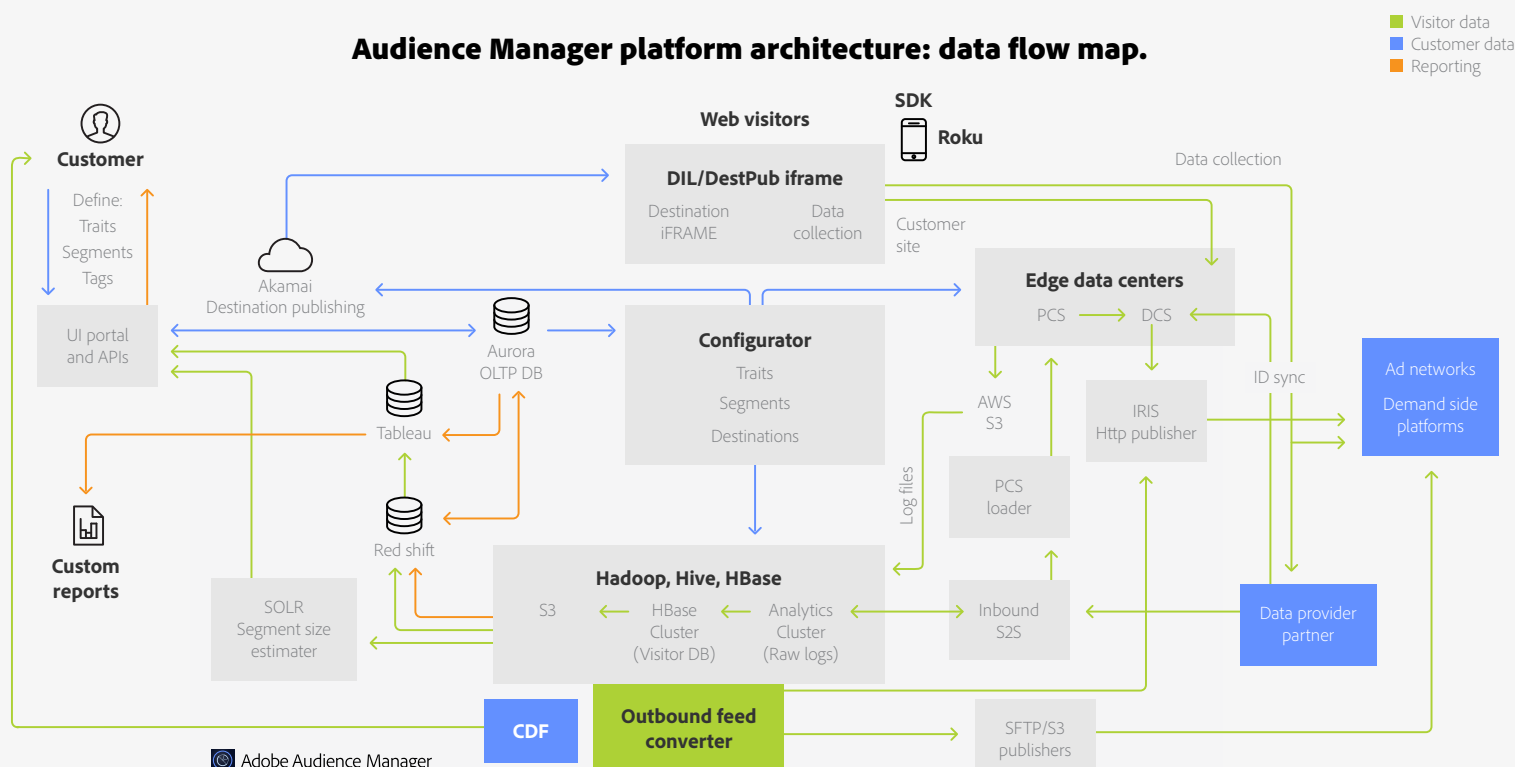
How does Audience Manager secure inbound and outbound data transmissions?

All Audience Manager data is encrypted in transit. It uses HTTPS 128-bit AES encryption when transmitting data over the Internet. Audience Manager encrypts inbound data using SFTP or AWS S3 for data on-boarding and HTTPS for real-time data collection. Outbound data sent server-side to external platforms is encrypted using SFTP or AWS S3 via HTTPS. For outbound data files, such as bulk exports and customer data feeds, Audience Manager uses either AWS S3 or SFTP (bulk exports only). Audience Manager also encrypts passwords, secret credentials, and some inbound at-rest partner data. More details are available in the Audience Manager data security documentation¹ and the Audience Manager Security Overview white paper.²

What are the data retention policies for Audience Manager?

Regulatory compliance concerns will often spur IT to ask about Audience Manager data retention policies. But this is also relevant to marketing teams that want the ability to target end-users through their destination partners. Actual retention lengths in Audience Manager vary based on data type and where it's being stored. As said, the retention of user data is what most IT and marketing teams are concerned about. Audience Manager deletes user data from its back-end servers after 120 days of no detected activity for a particular user. At 120-day period restarts whenever the system detects activity from that user. You can find more data retention details on the Audience Manager Data Retention FAQ.³

Audience Manager platform architecture: data flow map.



Points marketing and IT should consider together.

Should we take advantage of the Adobe Experience Cloud ID?

The Adobe Experience Cloud ID is a universal, persistent ID that can pseudonymously identify your visitors across all the solutions in the Adobe Experience Cloud. For example, if you also have Adobe Analytics, the Experience Cloud ID allows you to share segments between Analytics and Audience Manager, as well as send those segments to Adobe Target or Adobe Campaign to create connected, personalized customer experiences. The Experience Cloud ID also works in conjunction with the Adobe Experience Cloud Device Co-op, which can help you establish pseudonymous ties between the group of devices that individual customers use.

These pseudonymous ties help you get a holistic view of your customers' journeys across all their devices—without collecting any directly or personally identifiable data.

What Audience Manager implementation approach best fits our needs?

When deploying Audience Manager, you can choose either a client-side or server-side implementation. Adobe recommends the server-side implementation since it reduces the number of calls from the page, improves load times, and enables native integrations with Adobe Analytics and audience sharing with other Experience Cloud Solutions. However, there are a few requirements you need to meet in order to use a server-side implementation, including use of the Experience Cloud ID service and version 1.5 or later of the AppMeasurement.js, and VisitorAPI.js code libraries.⁴

How can Audience Manager help our teams with GDPR compliance?

Audience Manager is GDPR-ready and can support your efforts toward GDPR compliance. It gives you full control over how and what data is ingested into the Audience Manager. Since Adobe doesn't allow any DII data, any identifiable data needs to be converted into hashed IDs before it's ingested into Audience Manager for segmentation and activation.

To further aid your GDPR compliance efforts, Audience Manager includes data export controls that let you determine and control when data can or cannot be exported to a destination. Role-based access controls can help you ensure the right teams have access to intended data. Global opt-out management is available through both the Adobe Experience Cloud 1-click feature on the Your Privacy Choices page and a direct opt-out API call in Audience Manager. Additionally, when you map audience segments to third-party targeting partners, unsegmentation in Audience Manager can help you automate GDPR requests by flagging users who have requested to be removed.

To support compliance, it's a good idea for your marketing and IT teams (in consultation with your own legal team) to work together on the following:

- Review the various IDs you plan to use to identify users
- Consider using data export controls to block audience activation to technologies that house personal data
- Review identity linkage, privacy policies, and legal requirements to see when and where it's appropriate to tie identity sets together, and then do so using Audience Manager Profile Merge Rules

Visit our Adobe Audience Manager and General Data Protection Regulation (GDPR) webpage for more insights and help.⁵

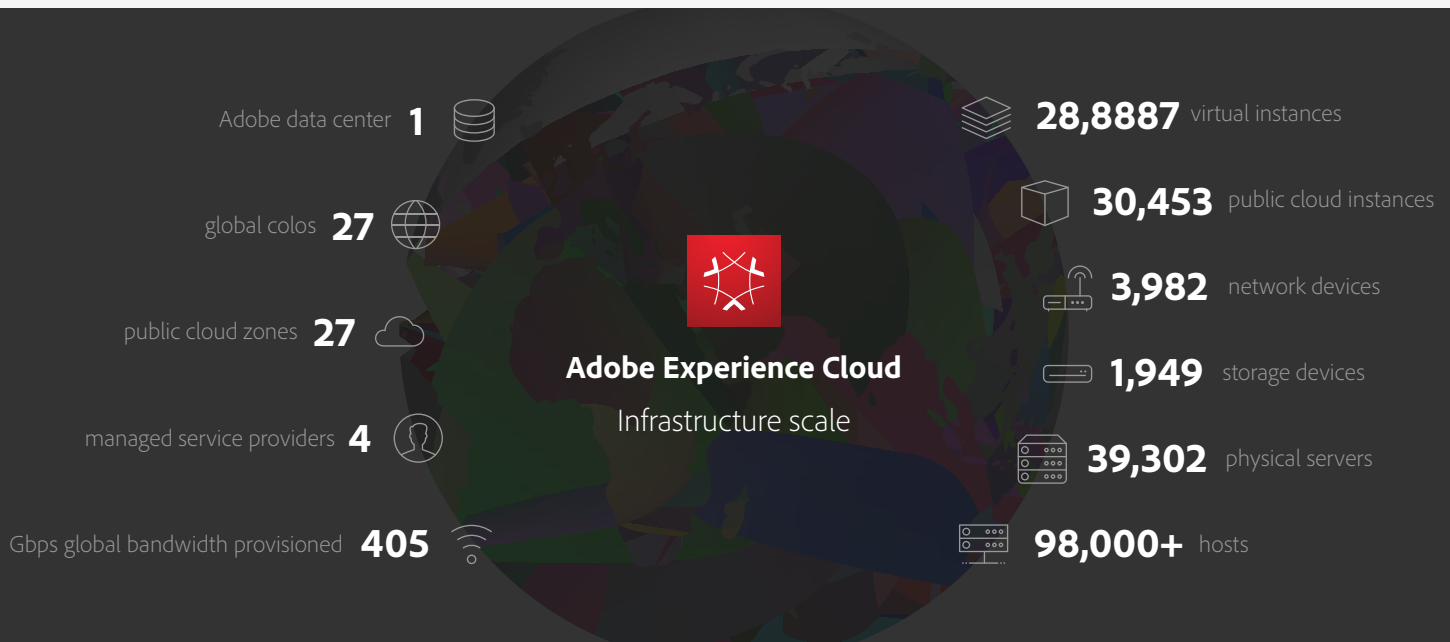
Adobe Audience Manager compliance.

- SOC 2—Type 2 (Security & Availability)
- ISO 27001:2013
- GLBA (Gramm-Leach-Bliley Act)-Ready
- GDPR (General Data Protection Regulation)-Ready

Note: An Adobe service that is GLBA-Ready, GDPR-Ready, HIPAA-Ready, FERPA-Ready, FDA 21 CFR Part 11-Compliant, or HIPAA-Ready means that the service can be used in a way that enables the customer to help meet its legal obligations related to the use of service providers. Ultimately, the customer is responsible for ensuring compliance with legal obligations, that the Adobe service meets its compliance needs, and that the customer secures the service appropriately.

Experience Businesses—those that consistently adopt CX best practices across people, process, and technology pillars—outperform their peers in business metrics spanning the entire customer journey. They also see topline gains, including **1.4x** revenue growth, **1.7x** customer retention rates, and **1.6x** customer lifetime value.⁶

TechOps chops.



We also processed over 70.8 trillion transactions for Audience Manager during 2017 alone.

For more information, visit the [Adobe Security site](http://www.adobe.com/security/compliance.html), www.adobe.com/security/compliance.html, and the [Adobe Trust Center](http://www.adobe.com/trust.html), www.adobe.com/trust.html.

¹ "Adobe Audience Manager Data Security"

² "Adobe Audience Manager Security Overview White Paper"

³ "Adobe Audience Manager Data Retention FAQ"

⁴ "Requirements for Server-Side Forwarding"

⁵ "Adobe Audience Manager and General Data Protection Regulation (GDPR)"

⁶ "The Business Impact of Investing in Experience," a commissioned study conducted by Forrester Consulting on behalf of Adobe, February 2018

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. Adobe, the Adobe logo, and the Adobe Experience Cloud logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.