

Contents

[About GDPR and why it matters](#)

[Adobe and data governance](#)

[Roles and responsibilities:
How Adobe supports brands' GDPR compliance](#)

[Key steps to GDPR readiness](#)

[Adobe Experience Cloud's
GDPR API: How it works](#)

[Example workflow:
Submitting GDPR requests to
Adobe Experience Cloud](#)

Adobe Experience Cloud and GDPR

Implementing the Adobe Experience Cloud GDPR API for streamlined GDPR requests^{*}

Adobe Experience Platform helps customers to centralize and standardize their customer data and content across the enterprise – powering 360° customer profiles, enabling data science, and data governance to drive real-time personalized experiences. Experience Platform provides services that includes capabilities for data ingestion, wrangling and analyzing data and building predictive models and next best action. Experience Platform makes the data, content, and insights available to experience-delivery systems to act upon in real time, yielding compelling experiences in the relevant moment. With Experience Platform, enterprises will be able to utilize completely coordinated marketing and analytics solutions for driving meaningful customer interactions, leading to positive business results.

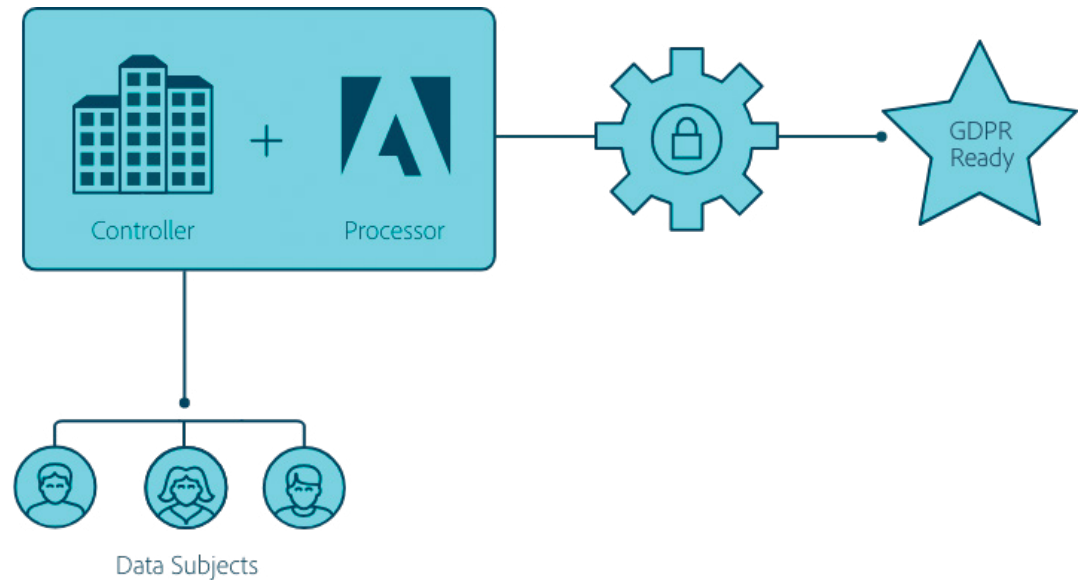
An integral part of Experience Platform is data privacy to improve experiences for our customers as they work to deliver real-time experiences through our open and extensible platform.

The way we look at it, data privacy (includes governance, data protection and consumer rights) is a key part of how brands create and sustain consumer trust. The deadline for GDPR compliance has arrived, consider it an opportunity to “lean in” to what Adobe Experience Cloud is all about —customer centricity and advancing the customer experience. Now is the time to reevaluate customer experience and customer journey best practices as they relate to data collection, transparency and consumer choice. In addition, preparing for GDPR and designing systems and policies with privacy in mind today is a smart investment in your brand's future — a necessity for global brands as well as any organizations that engage in digital marketing, particularly in highly regulated industries.

Adobe Experience Cloud's role as one of your GDPR data processors is to assist you in managing consumer data from across Adobe Experience Cloud Solutions to meet GDPR obligations. Adobe Experience Cloud already has a strong foundation of certified security controls and privacy by design. In addition, Adobe Experience Cloud has made enhancements to its products to support GDPR readiness, including developing an API for submitting GDPR processing requests to Adobe Experience Cloud. A key benefit of this GDPR API is that it enables brands to scale their response by handling potential high volumes of consumer information requests.

^{*} **Disclaimer:** This whitepaper is intended to provide general information and guidance and does not represent legal counsel. Seek the advice of your legal counsel for meeting the requirements in the regions where you operate.

This whitepaper will provide you with a brief overview of key GDPR principles important to data collection practices, suggest key steps to GDPR readiness, and set out the roles and responsibilities of brands that use Adobe Experience Cloud. In addition, you will find the technical documentation you need to implement the API in order to submit GDPR data requests to Adobe Experience Cloud.



Adobe Experience Cloud solutions supported by the GDPR API.

These are the solutions that interface with the GDPR API. For customers using other versions of Adobe Experience Cloud solutions (see notes below), please consult product documentation for information on GDPR readiness.

- Analytics Cloud
 - Adobe Analytics
 - Adobe Audience Manager
- Advertising Cloud
 - Adobe Media Optimizer
- Marketing Cloud
 - Adobe Campaign*
 - Adobe Experience Manager**
 - Adobe Social
 - Adobe Target
- Platform Services

* Refer to product-specific documentation to ensure that your version of Campaign interfaces with the GDPR API and to learn about tools or documentation for managing GDPR requests on those versions of Campaign that do not interface with the GDPR API.

** AEM instances and the applications that run on them are owned and operated by our customers; i.e., AEM customers function as both Data Processor and Data Controller. AEM will provide documentation and procedures for the customer privacy admin/customer AEM Admin to execute the GDPR requests manually or through APIs when available. Documentation will be provided for all impacted AEM Areas: AEM Sites, Forms, Communities, and Platform.

About GDPR and why it matters

The General Data Protection Regulation (GDPR) is the European Union's new privacy law that harmonizes and modernizes data protection requirements. The new rule has a broad definition of personal data and a wide reach, affecting any brand that markets products or services to individuals in the EU. GDPR goes into effect on May 25, 2018.

One of GDPR's key requirements is enabling consumers' rights regarding personal data a brand may have collected, including the rights to access and deletion.

There are four principles of GDPR that brands should consider as they review data collection practices related to Adobe Experience Cloud.

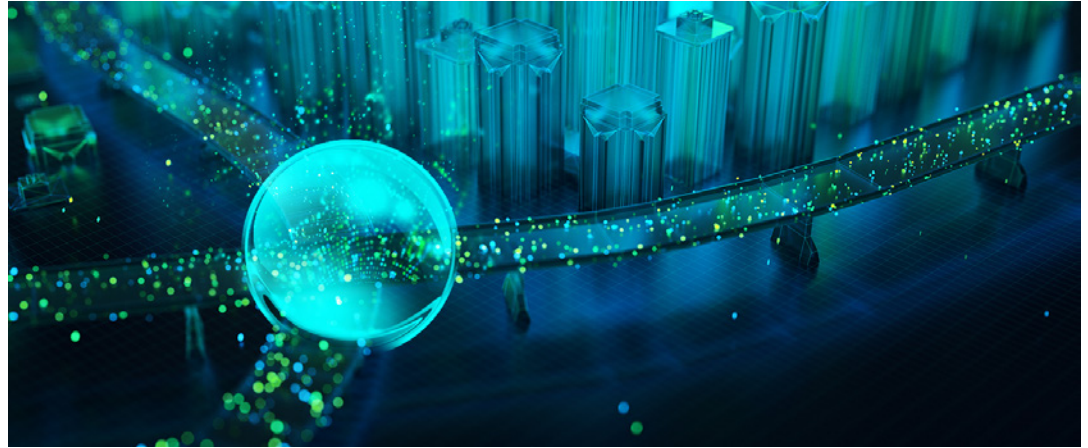
- 1. Focus on collecting only the data you need.** To be GDPR ready, it's important for brands to take stock of the data being collected and not collect more data than necessary.
- 2. Obtain appropriate consent.** GDPR is a good opportunity for brands to reconsider consent management strategy and practices. Under GDPR (and the related ePrivacy requirements), consent must be unambiguous and there must be a clear affirmative action by the site or app visitor. Consent also must be presented separately, easily understood and distinguishable from other content.
- 3. Remove personal identifiers where possible.** Brands should consider the role for privacy-enhancing techniques like data hashing, data obfuscation or data anonymization. Doing this will help minimize compliance obligations.
- 4. Honor data access and delete requests.** Consumers have certain rights related to the personal data brands collect and maintain about them, including the rights to access or deletion. To prepare to respond to these requests, brands should set data retention policies with their Processors, such as Adobe Experience Cloud. Applying appropriate, secure, and timely retention policies is an important part of GDPR readiness. Not only will this help address requirements related to not keeping data longer than necessary, but it will also assist in reducing the processing times associated with individual rights requests (e.g., consumer rights to access and delete personal data).



What is personal data?

According to GDPR, "personal data" is any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Adobe and data governance



The Adobe Experience Platform provides an integrated solution that connects a brand's data governance infrastructure with the tools it uses to create and manage consumer experiences. The data governance features of Adobe Experience Platform enable the direct linkage of data governance policy to data usage. Experience Platform, as a data and intelligence platform that enables all of Adobe's marketing and consumer experience solutions in Adobe Experience Cloud, centralizes the collection and storage of all consumer experience-related data and offers data governance actors (e.g., stewards, scientists, engineers, and marketers) the features they need to help define and enforce data governance rules that activate that data for the Experience Business. For more information about Experience Platform data governance features, see the [Adobe Experience Platform Data Governance whitepaper](#).



What is data governance?

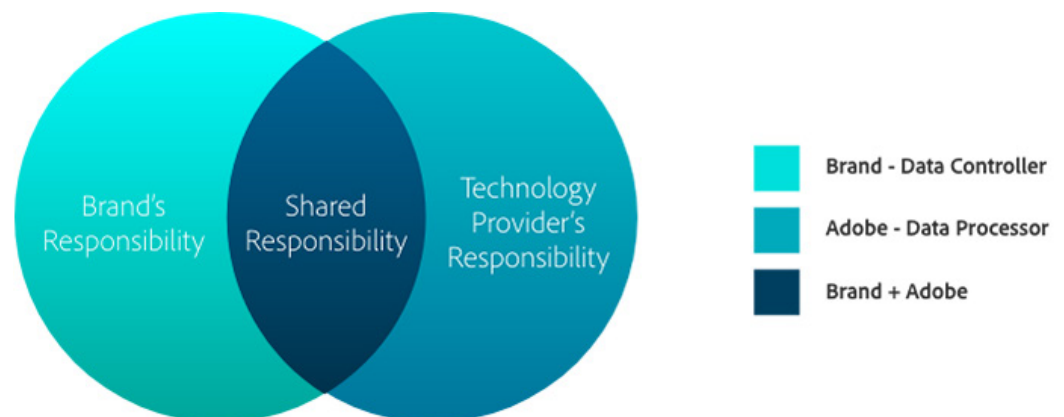
Data governance is having a system in place consisting of the people and digital tools required to exercise authority, control, and shared decision-making. It means creating a team to control data governance and giving that team the tools they need to govern data effectively and efficiently in real time. It encompasses both the strategies and the technologies required to ensure data and its use complies with the regulations, restrictions, and policies governing that use: data catalogs, data lineage, data usage labeling, data access policies, and more.

Roles and responsibilities: How Adobe Experience Cloud supports brands' GDPR readiness

GDPR sets out the obligations for the various parties involved with GDPR readiness. The obligation to meet the GDPR principles regarding data collection (see p.2) falls upon brands, also known as Data Controllers. However, the journey to GDPR readiness is in part shared between Data Controllers (brands) and technology vendors or Data Processors like Adobe Experience Cloud. There are three parties to become familiar with. Each of these parties is defined below within the context of Adobe Experience Cloud.



Adobe Experience Cloud's role is to help our customers (Data Controllers) respond to requests from their consumers (Data Subjects) when it comes to individual rights requests (e.g., access or delete requests) related to data maintained in the Adobe Experience Cloud.



You are the Data Controller. As the Controller, you determine the personal data Adobe Experience Cloud will process and store on your behalf. If you use Adobe Cloud Solutions, we may process personal data for you depending on the products and solutions you use and the information you choose to send to your Adobe account or service. As a Controller, you will provide privacy notices to individuals who engage with your brands detailing how you collect and use information, and obtain consents, if needed. If those individuals want to know what data you maintain about them or decide they want to discontinue their relationship with you, you will respond to those requests. You also are responsible for updating your brand's data governance, privacy and security policies and procedures.



We are the Data Processor. When Adobe Experience Cloud provides software and services to a brand, we're acting as a Processor for the personal data you ask us to process and store as part of providing the services to you. As a Processor, we only process personal data in accordance with your brand's permission and instructions—for example, as set out in your agreement with us. When your data is in one of Adobe's Cloud Solutions and you need our assistance with any individual consumer requests, we will partner with you through processes, products, services, and tools to help you respond.

Key steps to GDPR readiness

Although every brand will determine its own GDPR preparation strategy, we suggest that brands assess their GDPR readiness by thinking through five key steps. These include the following:

1. Inventory your digital properties, including mobile apps and websites, to assess which cookies, tags, or other data are necessary.
2. Map your customer journey and tell your privacy story through meaningful notices and choices.
3. Develop a consent management strategy with an eye toward customer experience.
4. Think about how you will authenticate user identity to address Data Subject access requests.
5. Identify or capitalize on existing processes to help respond to Data Subject access requests, including appointing a privacy point of contact.

GDPR puts increased emphasis on data collection best practices, transparency from Data Controllers, and consumer choice—all of which play a meaningful role in the customer journey. Some key considerations include the following:

 Topic	 Questions to ask
Data minimization	What data do I need and not need to collect for my marketing efforts to be effective?
Consent/opt-in	How do I provide delightful customer experiences with consent and without unwanted surprises? Consider the value proposition for consumer privacy, which will drive conversion and loyalty.
Required levels of notice and/or consent	Is notice enough? Is there another legal basis for certain data processing activities (e.g., product development and enhancements), such as legitimate interest, where you wouldn't need consent?
Anonymization and pseudonymization of data	How will we anonymize or pseudonymize personal data? Pseudonymizing data (i.e., replacing personal details with another unique identifier, typically generated through some kind of hashing, encryption or tokenization function) will minimize the risk of data and privacy breaches and claims. For example, "John Smith bought product X" could be pseudonymized to "Visitor 15436 bought product X."

Tip: Operate from the presumption that under the wide definition personal data much of the data you have is not anonymous (unless you take special privacy-enhancing measures). Think about a sliding scale based on the sensitivity of the data, which guides a risk-based approach.

Adobe Experience Cloud's GDPR API: How it works

Adobe Experience Cloud's GDPR API automates consumer GDPR access and delete requests across Adobe platform components. Overall, the process consists of three steps:



1. In advance of GDPR and as part of good data hygiene, the Controller should curate and label data in Adobe Experience Cloud Solutions.
2. Upon request of a consumer/Data Subject to learn what data the brand has or to delete their data, the Controller collects identities from the Data Subject, verifies that data and submits it via the Adobe Experience Cloud GDPR API.
3. Adobe Experience Cloud responds to GDPR requests and returns data to the Controller.

Using the GDPR API involves some up-front preparation on the part of brands. The following section outlines the technical documentation for these preparatory steps, as well as how to submit requests to Adobe Experience Cloud through the API.

Prepare for GDPR in four steps

1. Review Adobe Experience Cloud requirements.

Following are the basic requirements you must have in place to implement the GDPR API:

	Identify	Identify your organizations' Marketing Cloud Organization ID(s) (e.g., often called an IMS org ID such as 58303AC75434B69B0A4C98C6@AdobeOrg)
	Create	Create a new integration to the GDPR API through Adobe's IO Console (console.adobe.io).
	Define	Define your own API key (through the IO Console)
	Generate	Generate your own JWT tokens to exchange for an authorized access token according to the Adobe IO standards and documented process (https://www.adobe.io/apis/cloudplatform/console/authentication/gettingstarted.html)
	Leverage	Leverage an HTTP protocol tool to send requests to the API (CURL, Postman, etc.)
	Inventory	Inventory all Adobe Experience Cloud products you use and make sure you know if they are connected to your Marketing Cloud Organization ID(s), aka IMS Org ID. If any products are not connected with a Marketing Cloud Organization ID, then note the legacy organizational ID for that product. This is important because a GDPR request needs a single Marketing Cloud Organization IDs followed by multiple legacy org IDs. You could have multiple Marketing Cloud Organization IDs and if you wish to address data stored under any of those IDs, you must submit a separate request for each Marketing Cloud Organization ID. If a brand only has legacy org IDs and no Marketing Cloud Organization IDs, then you will need to talk to your Customer Success Manager or to Adobe Customer Care to be provisioned with a new Marketing Cloud Organization ID, which will allow you to issue GDPR requests via the API.
	Curate	Curate your data in Adobe Application Manager (AAM) if relevant. Organize a process to obtain Data Subject identity mapping to Adobe identifiers when using onboards or hashing mechanisms (e.g., hashed CRM ID in AAM).

2. Curate and label your data.

Before sending GDPR requests to Adobe Experience Cloud, you must identify what personal data Adobe Experience Cloud should process and store on your behalf. This involves going into Adobe Experience Cloud products or services in which you house complex data types (e.g., Adobe Analytics, Platform, or Campaign) to identify and label the data types that should be referenced in a GDPR request. This is the Controller's responsibility because data schemas will vary by customer and Solution.

When you identify fields that contain any GDPR-relevant data, you should label the data or consider using the general data governance labels in Adobe Experience Platform's Data Usage Labeling & Enforcement (DULE) framework when available. The DULE features enable data stewards to apply labels (metadata) to data, either as it's ingested or after, and categorize it according to what kind of data usage policies apply to it. For more information about the DULE framework, please see the Adobe Experience Platform Data Governance whitepaper.



How to label data: An example.

Let's say the Controller plans to collect cookie IDs from Data Subjects to process their GDPR requests. These cookie IDs are stored in a Report Suite in Adobe Analytics. To create a label for cookie IDs, the Controller must supply their own label of his/her own or use Adobe Cloud Platform's Data Usage Labeling & Enforcement (DULE) framework in Analytics (if available). The Controller then takes the label from this activity and codes it as an API parameter in Adobe Experience Cloud's GDPR API. When Adobe Analytics receives this GDPR request from the API call, it can identify that the supplied data refers to a cookie ID in a particular Report Suite, and return that data or process the deletion.



Data Subjects

Adobe Experience Cloud's customers' consumers



Data Controllers


Adobe Experience Cloud's customers



Data Processor

Adobe Experience Cloud

Data curation in Adobe Analytics: Creating labels for columns in a fictitious Analytics Report Suite to activate it for GDPR-requests processing.





Determining what is "personal data."

Examples of personal data that can be sent to Adobe Experience Cloud include name, email address, certain persistent identifiers, and IP addresses. For a more detailed list of examples, see <https://www.adobe.com/privacy/marketing-cloud.html#collect>.

3. Set up your Data Subject user portal and deploy Adobe Experience Cloud's JavaScript library.

The Adobe Experience Cloud JavaScript (AdobePrivacy.js) is a lightweight JavaScript library that helps you collect different types of Adobe cookies in a format compatible with how our solutions identify data categories. Controllers can choose to deploy AdobePrivacy.js on the portals where they interact with Data Subjects. AdobePrivacy.js enables you to more easily collect relevant IDs so that you can submit these identities as part of access and delete requests via the GDPR API. For certain workflows in solutions such as Adobe Advertising Cloud, the JavaScript library completes a GDPR delete request within the user's browser by deleting relevant Adobe cookies on the client side (i.e., from the same browsing session). For more information, see [documentation](#) for the JavaScript library.

The AdobePrivacy.js enables two methods for the Controller to call:

 retrieveIdentities (callback)	Use to collect IDs for access and delete requests
 removeIdentities (callback)	Use to remove IDs from the browser for delete requests

It is important to note that AdobePrivacy.js is not consumer-facing—that is, website or app visitors will not submit requests directly to the Adobe Experience Cloud GDPR API. Rather, the consumer IDs collected by the Controller need to be submitted by the Controller via the Adobe Experience Cloud GDPR API. Also, please note that AdobePrivacy.js only needs to be deployed on your privacy portal. It is not needed anywhere else on your website.

Following are steps to AdobePrivacy.js implementation, if you have decided to set up a privacy portal to interact with Data Subjects to receive GDPR requests:

1. Add AdobePrivacy.js to your Data Subject privacy portal.
2. Implement callback for "retrieveIdentities" and store the result in your system until you are ready to submit to Adobe Experience Cloud.
3. Also call "removeIdentities" for delete requests.
4. Self-host AdobePrivacy.js if required.
5. Start process of security approval, if needed, to implement AdobePrivacy.js. Engage the right stakeholders; e.g., conduct a security and privacy review, according to your organization's policies.

4. Determine how you will enable consumer data requests.

If consumers/Data Subjects want to know what data you maintain about them or decide they want to discontinue their relationship with you, the Controller is responsible for responding to those requests. The Controller determines how the organization will interact with Data Subjects (e.g., through a Data Subject privacy portal) and manages interactions with the Data Subject. It also is your responsibility to close the loop with the Data Subject when the request is fulfilled. In other words, Adobe Experience Cloud, as the Data Processor, will not be receiving requests directly from Data Subjects—only from Data Controllers.

You also may want to ensure your mobile apps and websites will provide relevant notices and supporting materials about consumers' rights regarding their personal information.



Consumer consent management

You will need to provide privacy notices to individuals who engage with your brand detailing how you collect and use information and obtain consents, if needed.

Adobe Experience Cloud currently does not offer a consent management solution.

A list of some of the emerging privacy vendors in this space, some of which offer consent products, can be found at: https://iapp.org/media/pdf/resource_center/2018-Privacy-Tech-Vendor-Report-V2.1e.pdf.

Example workflow: Submitting GDPR requests using Adobe Experience Cloud GDPR API

Following is an example workflow for clarification purposes only. Its purpose is to help brands understand how a GDPR data request workflow could be structured. This is not a specific recommendation of how a brand should structure its GDPR data request workflow.

1. Data Subject Laura submits access/delete request via Brand X's privacy portal or other mechanism or UI set up to accept GDPR requests from the Data Subject
2. Brand X's privacy analyst Ann collects details from Laura that are necessary to execute a GDPR request to Adobe Experience Cloud (e.g., using Adobe Experience Cloud GDPR JavaScript), including obtaining IDs about Data Subject Laura
3. Ann submits Laura's request and Data Subject IDs via integration with Adobe Experience Cloud GDPR API.
4. Adobe Experience Cloud processes Laura's request, finds relevant data in Adobe Experience Cloud Solutions, returns the data to Ann or deletes it, and returns a receipt of deletion to Ann.
5. Ann reviews the data returned by Adobe Experience Cloud, per a pre-determined internal process to ensure the request was processed correctly
6. Ann then returns the relevant requested data or confirmation of deletion to Data Subject Laura.

Submit data requests via the Adobe Experience Cloud GDPR API



Integrating with the GDPR API helps Data Controllers orchestrate data collection across the majority of Adobe Experience Cloud Solutions. In response to a query, we, as the Processor, help you find relevant data in our Solutions based on the identities you've supplied to us. If it's an access request, we return an archive of the data that was found. If it's a request to delete, we delete it and return a receipt of deletion.



Note:

Controllers can make a single API call to submit multiple identities across multiple Adobe Experience Cloud Solutions. However, each API call can only have a single Marketing Cloud Organization ID. If you have multiple Marketing Cloud Organization IDs, you must make multiple API calls. This is because the API identifies an organization using Marketing Cloud Organization IDs for security purposes.



Regarding legacy org IDs:

If you have legacy organizational IDs, such as with Campaign and Advertising Cloud, you must enumerate these organizational IDs with help from Adobe Customer Care if needed. When you make an API call, you should supply one Marketing Cloud Organization ID (aka IMS Org ID), followed by zero or more legacy org IDs.



Important reminder:







It's a good idea to make it clear to consumers/Data Subjects that access/delete requests are treated on a per-device basis. Therefore, a Data Subject must make separate access/delete requests to your brand from each of his/her devices (e.g., mobile, laptop, desktop, tablet).

Following are steps to prepare for submitting GDPR requests using HTTP, as well as more detailed information about the GDPR API.

To submit GDPR requests, follow these steps:

- Obtain an IMS user access token
 - Follow instructions for exchanging your JWT token (from your IO Console integration) with an access token (https://www.adobe.io/apis/cloudplatform/console/authentication/jwt_workflow.html)
- Find your Marketing Cloud Organization ID
- Assemble request header:
 - x-gw-ims-org-id: <org ID>
 - x-api-key: <obtained from Adobe IO Console integration>
 - Authorization: Bearer <token from first step>
- Assemble request body
 - Mandatory fields
 - Company context
 - IMS org ID
 - Other legacy account identifiers if necessary
 - User ID collections
 - Contain a unique user identifier (key)
 - Action type per user (access/delete)
 - Collection of:
 - Qualifying namespaces (i.e. "email")
 - Values
 - Types
 - Optional—any exclusions by product name
- Submit request and capture return data (job ID's per user)
 - Make an HTTP request to API programmatically or download/access an HTTP utility and submit a request

Following is more detailed information about the Adobe Experience Cloud GDPR API. The resource path for all requests to the service is: <https://platform.adobe.io/data/privacy/gdpr>. The following method types are listed below:

 API Name	 Method type	 Path	 Description	 Input Parameters	 Response
Access/Delete	POST	/data/privacy/gdpr	Create one or more ACCESS or DELETE requests to retrieve or delete all data corresponding to the provided user ID's	<p><i>Header:</i></p> <p>x-gw-ims-org-id: <org ID originating request></p> <p>x-api-key: <application key for Adobe IO></p> <p>Authorization: Bearer <token></p> <p><i>Content-Type:</i></p> <p>application/json</p> <p><i>Body:</i> See JSON body below</p>	<p>202 Accepted</p> <p>400 - Bad request - if the JSON body fails to process properly</p> <p>500 - Server error - unforeseen service issues</p>
Status	GET	/data/privacy/gdpr/{jobid}	Retrieve the status of a job	<p><i>Header:</i></p> <p>x-gw-ims-org-id: <org ID originating request></p> <p>x-api-key: <application key for Adobe IO></p> <p>Authorization: Bearer <token></p> <p><i>Content-Type:</i></p> <p>application/json</p> <p><i>Path parameters:</i></p> <p>jobid - returned from an Access/Delete request</p>	<p>200 success - JSON body with data regarding the status of the job</p> <p>404 Not Found</p> <p>406 Not acceptable - format not supported</p> <p>500 - Server error - unforeseen service issues</p>
Status (all)	GET	/data/privacy/gdpr	Retrieve status of all jobs for the requesting user	<p><i>Header:</i></p> <p>x-gw-ims-org-id: <org ID originating request></p> <p>x-api-key: <application key for Adobe IO></p> <p>Authorization: Bearer <token></p> <p><i>Content-Type:</i></p> <p>application/json</p> <p><i>Query parameters (optional):</i></p> <p>startdate - day to begin job search</p> <p>enddate - day to end job search</p>	<p>200 success - JSON body with records from audit table</p> <p>404 Not Found - no jobs within the scope of the requesting user</p> <p>406 Not acceptable - format not supported</p> <p>500 - Server error - unforeseen service issues</p>

Data submission format

Data submission formats are detailed below.

```
{
  "companyContexts": [{
    {
      "namespace": "imsOrgID",
      "value": "123456789@AdobeOrg"
    },
    {
      "namespace": "AdCloud",
      "value": "AdvId:12345"
    },
    {
      "namespace": "Campaign",
      "value": "acme-stg-us1"
    }
  ],
  "users": [{
    {
      "key": "David Smith",
      "action": ["access"],
      "userIDs": [{
        {
          "namespace": "email",
          "value": "dsmith@acme.com",
          "type": "standard"
        },
        {
          "namespace": "myCustomField",
          "value": "myCustomId_1234",
          "type": "unregistered"
        }
      ]
    },
    {
      "key": "Alicia Jones",
      "action": ["access", "delete"],
      "userIDs": [{
        {
          "namespace": "email",
          "value": "ajones@acme.com",
          "type": "standard"
        },
        {
          "namespace": "411",
          "value": "123ab4de32114bb001",
          "type": "namespaceId"
        },
        {
          "namespace": "loyaltyAccount",
          "value": "222050656788",
          "type": "custom"
        },
        {
          "namespace": "reportId",
          "value": "276AD",
          "type": "integrationCode"
        }
      ]
    }
  ],
  "exclude": ["Analytics"]
}
```

Some notes about the format:

- The key is a user identifier to wrap the various namespace entries and is used to qualify the separate job IDs in the response data, largely used by the data controller for reference and grouping and may be any string value.
- The action field is a collection of desired actions, one or both of ["access" | "delete"] depending on the user's request, and may be different for each user in the submission.
- The combination of key and action dictate how many "jobs" are created in the service to track. A user key with a single action creates a single job, but a user with both an access and delete request will generate two separate jobs against that user key. Multiple keys in a file (indicating multiple user ID collections) will generate multiple jobs as well.
- As mentioned above, users may have 1 or many JSON sub-documents including namespace, value and type that represent their identity in the ExC.
- The namespace and type fields are detailed in the table Namespace Qualifiers below.
- The number of userIDs under each user while creating jobs for users is limited to 9. For example, the API will support accepting up to 9 userIDs under each user.
- The include key is an optional parameter and supports an array of product strings to exclude in your processing. If you only support or integrate with Analytics, you could include only Analytics in the request. By default, all supported ExC solutions are included in every request. See product values.

One key not detailed in the example above:

- The key isDeletedClientSide is a Boolean (true/false) value that is handed in from Adobe's Privacy JS library, indicating the client-side cookie has been deleted. This flag resides at the userID level, as part of the namespace, value and type triumvirate, and should not be added to the request manually as it indicates additional processing work is not needed by some solutions.

Conclusion

GDPR compliance can be a brand-building opportunity to advance customer centricity and customer experience. It is also a way for brands engaged in digital marketing to future-proof data privacy systems and policies, particularly for global brands and organizations in highly regulated industries. Another way to look at it is to see that consumer consent and opt-in can be a new KPI to measure customer engagement, loyalty, satisfaction, and trust—music to a marketer's ears. Although GDPR readiness is a complex undertaking, Adobe Experience Cloud is ready to support our customers in streamlining GDPR data requests for Adobe Experience Cloud Solutions.

For additional information, see

<https://www.adobe.com/privacy/general-data-protection-regulation.html>

For any additional questions contact askprivacy@adobe.com.



Adobe Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Incorporated in the United States and/or other countries.
All other trademarks are the property of their respective owners.
© 3/2018 Adobe Incorporated. All rights reserved. Printed in the USA.