THE GENERAL DATA PROTECTION REGULATION (GDPR) AND YOUR BUSINESS

A care package to help you get GDPR-ready with Adobe Experience Cloud
Table of Contents

3-4  Introduction to GDPR

5-6  Adobe is here to help

7    Tips & Tricks to GDPR Readiness

8    Common GDPR Myths

9-10 Frequently Asked Questions
Introduction to GDPR

This document on GDPR will give you the foundational understanding you need to help you on your journey towards GDPR readiness.

GDPR Modernizes Data Protection Requirements

The European Union’s General Data Protection Regulation (GDPR) is a privacy regulation that harmonizes and modernizes data protection requirements. The new rules have a broad definition of personal data and a wide reach, affecting any company that markets products or services to individuals in the EU. Among other things, GDPR provides for enhanced rights of individuals, who can ask companies to access, correct or delete their personal data, and object to any future data collection. We believe GDPR presents an opportunity for businesses to strengthen their brand loyalty by focusing on consumer privacy while delivering amazing experiences. Think of it as experiential privacy – having privacy be a key part of the customer experience.
Brands should take this opportunity to review data collection practices and consider the following:

**Focus on collecting only the data you need:**
Take stock of the data being collected, and do not collect more data than necessary. Collecting only the needed data to drive your marketing campaigns, as opposed to collecting all the data you can, will not only serve you well from a business perspective, but will also help you to comply with privacy requirements.

**Obtain appropriate consent:**
GDPR is a good opportunity to re-consider your consent management strategy and practices, including determining when consent is needed and thinking about the value proposition for the user. Under GDPR (and the related ePrivacy requirements), consent must be unambiguous and a clear affirmative action by the site or app visitor. It also must be presented separately, easily understood and distinguishable from other content.

**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 your compliance obligations.

**Honor data access and delete requests:**
Consumers have certain rights related to 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 data processors, such as Adobe. 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).

**Provide the required notice for data collection:**
Review and update your current privacy notices, policies, and any information provided at data collection points.
There are three parties to become familiar with when it comes to GDPR. Each of these parties is defined below within the context of Adobe Experience Cloud.

Adobe is here to help

Adobe's GDPR capabilities provide you with what you need to respond to GDPR requests regarding your data stored in certain Adobe Experience Cloud solutions.

Adobe either already meets or is implementing its obligations as a Data Processor. We have a strong foundation of certified security controls and a heritage of privacy by design. We continue to update our products and services to be able to better partner with Data Controllers to move towards GDPR readiness. As one of your Data Processors, Adobe built a series of data privacy features in Adobe Cloud Platform to help you become GDPR-ready with Adobe Experience Cloud Solutions.
Key Capabilities
Adobe built the following data privacy features in Adobe Cloud Platform to help you become GDPR-ready with Adobe Experience Cloud solutions.

- **SUPPORT ANY VOLUME OF REQUESTS**
The open GDPR API is designed to process individual rights requests (e.g., access and delete requests) for our customers’ data stored across Adobe Experience Cloud solutions. It is flexible and scales according to the number of data access and delete requests your company receives from Data Subjects.

- **GET STATUS UPDATES, ANYTIME**
Monitor progress on how the data access and delete requests are being fulfilled.

- **COLLECT ADOBE IDs WITH EASE**
Adobe’s GDPR ID retrieval tag is a light JavaScript file that finds and easily captures user IDs across Adobe solutions. It is available in raw JavaScript, or as a pre-built integration in Launch by Adobe, our new tag management system.

- **BACKWARDS COMPATIBLE**
The GDPR API can support a broad range of customer IDs across both current, and legacy Adobe solutions.
Tips & Tricks to GDPR Readiness

Discuss with your Legal Team the following tips & tricks to help you become GDPR ready.

**INTEGRATE WITH OUR GDPR API**
The GDPR API will help you facilitate and scale the processing of individual rights (e.g., access and delete requests) for your data stored across certain Adobe Experience Cloud solutions.

**CONSIDER DEPLOYING GDPR ID RETRIEVAL TAG TO CAPTURE USER IDs**
Your development teams will save time by using our GDPR ID retrieval tag to capture user IDs, and then using our GDPR API to send those user IDs to the relevant solutions in the Adobe Experience Cloud for GDPR request processing. The GDPR API can support a broad range of customer IDs across both current, and legacy Adobe solutions.

**CONSIDER UPDATING YOUR ACP SDKs**
You can use the Adobe Cloud Platform SDKs (formerly known as the Adobe Mobile SDK) to support GDPR retrieve and delete requests from your mobile apps. GDPR is supported only in version 4.15 or later.

**START WORKING ON CONSENT SOON**
Strengthen consumer relationships by implementing a consent strategy that aligns with your larger marketing strategy, and with GDPR.

**FIND A CONSENT MANAGEMENT TOOL**
A consent management tool helps you obtain and manage consumers’ consent to track behavioral data, and use it for certain purposes. Adobe does not currently offer a consent management tool. Customers that use Launch by Adobe can leverage the prebuilt integrations from Evidon, TrustArc, and OneTrust.
There’s quite a bit of misinformation when it comes to GDPR. This page is dedicated to debunking those myths.

**GDPR dictates that data must stay in Europe.**
Not true. GDPR requires that the privacy protections afforded to European data flow with it wherever is transferred or accessed. Visit the Adobe Privacy Center to learn more about how Adobe addresses data transfers: [https://www.adobe.com/privacy/eudatatransfers.html](https://www.adobe.com/privacy/eudatatransfers.html)

**GDPR only applies to European companies.**
GDPR is not only applicable to companies based in Europe. GDPR it could apply to any company, no matter where its headquarters are, that offers goods and services or markets to individuals in the EU.

**Marketers will need to get all new consents for their marketing database.**
GDPR changes how brands obtain consent and may require some consents to be refreshed or updated. For instance, if a brand’s current consent practices meet or exceed the obligations outlined by GDPR then no changes to consent may be needed. However, if a brand’s consent practices fall short of the enhanced obligations, then those consents should be reevaluated and modernized.

**Marketers need consent for everything.**
Marketers don’t necessarily need consent for everything and this will depend on the nature of the data collection practices. There is some scope to rely on other bases for processing, like legitimate interest, for certain marketing activities. Companies should work with their counsel to explore the best approach to support their marketing initiatives.
Frequently Asked Questions

We know you probably have many questions. Below are a few commonly asked questions, and their answers.

My business is headquartered outside of Europe, does GDPR apply to us?

Potentially, if you market products or services to individuals in the EU and you collect personal data, then GDPR may impact your business.

What is my role as a Data Controller?

As the Data Controller, you determine the personal data Adobe processes and stores on your behalf. If you use Adobe Experience 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 Data 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 at some point during the consumer lifecycle those individuals want to know what data you maintain about them or decide they want to discontinue their relationship with you, you will need to have mechanisms in place to respond to those requests.
What steps do brands should consider to become GDPR-ready?

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 towards customer experience.
4. Determine how you will authenticate user identity to address data subject requests.
5. Identify and capitalize on existing processes to help respond to data subject requests.

The consent management space (e.g., tools, standards, best practices) is rapidly evolving, and is an area to watch. To minimize impact on user engagement, Data Controllers should work with vendors in this space and with their counsel, and follow emerging EU laws and guidance on consent and cookies. Thinking about “experiential privacy” by using an on-brand, contextually relevant experience that sets out the value proposition of your data collection activities is a good strategy.

What is Adobe’s role as a Data Processor?

When Adobe provides software and services to an enterprise, like yours, Adobe is acting as a Data Processor for the personal data you ask us to process and store as part of providing the services to you. As a Data Processor, we only process personal data in accordance with your company’s instructions — for example, as set out in your agreement with us. If your data is in one of Adobe’s 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.

How should Data Controllers think about consent when it comes to user engagement?

Frequently Asked Questions
Technical Documentation
For detailed technical documentation, go to https://www.adobe.io/apis/cloudplatform/gdpr/docs.html.