FREQUENTLY ASKED QUESTIONS

Adobe & the General Data Protection Regulation
What is the General Data Protection Regulation, or GDPR?

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 now ask companies to access, correct or delete their personal data, and object to any future data collection. We believe GDPR presents an opportunity for marketers 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.
When did GDPR go into effect, and what’s the penalty for non compliance?

GDPR went into effect on May 25, 2018. The penalty for non-compliance is up to 4% of annual revenue.

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

Potentially, if your business markets products or services to individuals in the EU then GDPR may apply to your business.

Whose responsibility is it to become GDPR ready?

GDPR is a shared compliance journey, with the regulation setting out the obligations for the various parties. The example below from Adobe Experience Cloud sets out the roles for brands or “data controllers”, technology providers or “data processors”, and the places where the data processor may need to help or partner with the data controller either through tools, processes, or documentation to help the data controller.
In the context of Adobe Experience Cloud, Data Controllers are Adobe’s customers. They own and control the personal data they house about their consumers (Data Subjects).

Adobe Experience Cloud is a Data Processor. Adobe processes personal data based on the permission and agreement we have with, and at the direction of, our enterprise customers (Data Controllers).

Adobe either already meets or is implementing our 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. Because GDPR is a shared responsibility between Data Controllers and Data Processors, enterprise customers will need to implement these product enhancements, as well as update any necessary policies and procedures, to become GDPR-ready.
What is Adobe's role as a Data Processor?

As the Data Processor, 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 Processor, 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.

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.

What steps should brands 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.

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.

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.

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.

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.

What steps should brands 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.
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. Consider the value proposition for consumer privacy, which can help drive conversion and loyalty.

**Provide the required notice for data collection:**
Review and update your current privacy notices, policies, and any information provided at data collection points.

**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).
Will customers (Data Controllers) need to submit multiple requests to Adobe Experience Cloud if they use more than one product (i.e. AA, Target, AAM, Campaign)?

For most customers, the answer is no since GDPR requests for Adobe Experience Cloud products and services will go through our Adobe Cloud Platform GDPR API or UI before being processed by the solutions and services to which the customer is entitled to, e.g, Adobe Analytics, Adobe Audience Manager (AAM), Adobe Target, Advertising Cloud (AdCloud), or Adobe Campaign Standard (ACS). However, you might need to submit a separate request to Adobe Campaign Classic since it has a separate API & UI for GDPR requests processing. Please, note that on-premise or managed instances of Adobe Campaign and Adobe Experience Manager (AEM) are not connected to the GDPR API.

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.

GDPR doesn't prohibit transfer of data outside of Europe. 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

Yes, the data is browser and device specific. As a result, separate requests need to be made to access and/or delete the corresponding data.

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

Does GDPR prohibit transfer of personal data outside of EU region?

If a Data Subject has accessed my site from multiple browsers or devices, does it need to make a request for each browser or device?