



EXPERIENCE CLOUD

Data privacy is all of our business.

An introductory guide.





Overview

Information and technology are fundamental to how the world connects today and responsible, transparent use of consumer data is now table stakes for organisations across the globe. Delivering customer experiences with privacy in mind has become a necessary investment given the dynamic nature of global privacy laws, technology and consumer expectations. Organisational missteps can potentially erode both customer trust and brand reputation. On the other hand, maintaining a trusted reputation with customers unlocks an ongoing relationship that encourages them to align their interactions and spending with brands that represent their own values.

“Trust is paramount,” says Clint Eagar, senior technical product manager at ObservePoint, an Adobe partner in the analytics management and tag governance space. “In our day and age, there are so many options out there. If a customer can’t trust us with their data, then they shouldn’t be doing business with us.”

Delivering privacy-conscious experiences is an important responsibility of many within an organisation. This isn’t a one-person job, nor is there a one-size-fits-all approach to address evolving legal compliance requirements, consumer

expectations and business needs. So, whether you're a member of the C-suite, a legal or IT professional, a marketer, data security or any other party that manages customer data, there's a seat for you at the table.

As we step closer to a world without third-party cookies and as consumers expect and demand more of a say in how organisations use their data, a user-centric approach to privacy and a flexible set of data governance solutions are needed. This approach will help you establish and manage consumer information in a way that builds trust, creates a positive experience and keeps your organisation ready for industry regulations.

At Adobe, privacy and security are intentionally and thoughtfully designed into the development of our enterprise tools and services. In an effort to contribute to and expand the conversation, we're sharing how Adobe solutions could fit within your own approach to privacy. While more detailed and technical documentation is available on this subject, this guide will help you get oriented. And while we understand that what works for us may not necessarily work for your organisation, we hope it will help in your efforts to organise and manage data privacy and governance more effectively.





Privacy in the enterprise.

Adobe provides customers with tools and technologies that enable them to deliver responsible, privacy-focused and user-centric experiences that align with consumer expectations. However, it's each organisation's responsibility to comply with the regulations as they apply to them.

What you do with consumer data as an organisation depends on what you're using the data for, how you're communicating the usage with your customers and what points of compliance you need to meet. Make sure you include business, legal, security, product and other key stakeholders when defining your organisation's privacy needs and values.

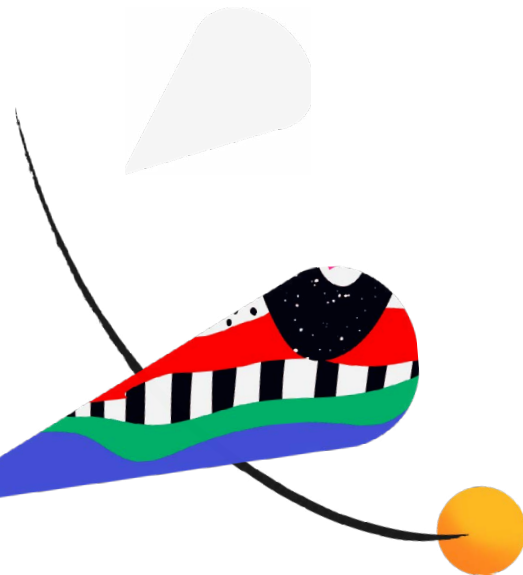
The most successful organisations consider why they're collecting the data and the benefit to the consumer. It's important to ask if you really need that data. Are you and the consumer getting value from the data you're collecting? Having the right values in place help you stay ready for new regulations.

"What I hear often is, 'I have to do this because it's regulated.' Well, that's not entirely true," says Elizabeth Sexton, senior product manager for Adobe Experience Platform at Adobe. "Regulations don't always say how you have to do it. They just say you have to do it. You have to make some decisions along the way."

We developed [Adobe Experience Platform Privacy Service](#) to help you respond to individual rights requests under regulations like General Data Protection Regulation (GDPR) and California

Consumer Privacy Act (CCPA). Privacy Service provides a RESTful API and user interface to help you manage data requests you receive from your customers – like accessing or deleting personal data from Adobe Experience Cloud applications in accordance with legal and organisational privacy regulations. As new privacy regulations come into effect, we'll continue to evaluate additional service functionality to help support your need to meet these new requirements.


As a brand, you understand best what data you need and the privacy requirements you need to follow. To help you understand what we do and do not support from a privacy regulation standpoint and individual rights request, we've compiled a [list of applications](#) that are integrated with Privacy Service.





Privacy in product development.

At Adobe, we treat data privacy as a fundamental design principle for our enterprise products. We proactively incorporate certified security controls and tools into product development to help brands manage their data, and to empower them to be flexible enough to meet regulations and adhere to their own privacy values using our tools and services.



A lot of my focus is spent on making those end-to-end experiences flexible so brands can implement privacy in the way that works for them,” says Sexton. “Because they control the data they collect.”

Elizabeth Sexton

Senior Product Manager for Adobe Experience Platform,
Adobe



According to The Forrester Wave™: Data Management Platforms, Q2 2019, “Adobe’s product differentiates as it is built on the principles of Privacy by Design and holds numerous vertical-specific security certificates that allow it to handle customer data in highly regulated industries like healthcare and financial services.”

Adobe Experience Platform allows you to unify all your data into robust customer profiles that update in real time. It's the foundation of Adobe Experience Cloud products and helps you deliver the right experience across every channel. It also supports technology and solution partners as they build and integrate their own products and technologies. It's built in a way that gives you the controls you need to manage customer data and ensure compliance with data regulations, restrictions and policies across Adobe applications.

To help manage your data to meet your obligations and your customers' expectations, you need a way to help identify each individual. One method is through the use of Experience Cloud Identity Service (ECID). ECID provides a universal and persistent ID that allows you to connect your visitors across Adobe Experience Platform applications. By having a common identifier within Experience Platform for each visitor, brands can more easily synchronise their data with partners (either their own or those who have integrated with Experience Platform) and connect with their offline or other IDs.

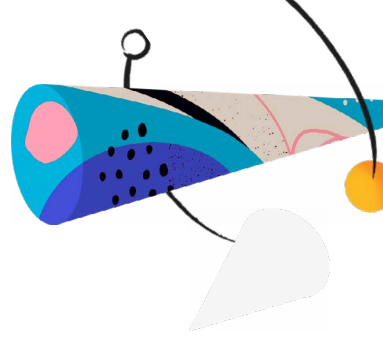
In order to more easily process consumer requests for their data – including access, delete, opt-in and opt-out requests – each consumer needs to have a unique identifier. Otherwise, it can be difficult to reconcile their many interactions with a brand across multiple channels. ECID is a great way to make sure that consumer data is used for its intended purpose across Adobe applications, allowing brands to better track the permissions they've received from consumers on how their data can be used. For more about ECID read the [overview](#).

Our [Real-time Customer Data Platform](#) (Real-time CDP) application service also helps you better identify, understand and engage your consumers. It's been designed with privacy in mind as well. Real-time CDP is a registered vendor in the IAB Transparency & Consent Framework (TCF). In compliance with TCF 2.0 requirements, it allows you to collect detailed customer consent data that is part of the TCF consent string and integrate it with your stored customer profiles. It can then be factored into whether certain profiles are included in exported audience segments.

Adobe also has a Privacy Customer Advisory Board to help vet new tools and discuss industry issues. We value our enterprise customers and want to make sure we're continually developing applications that serve their privacy needs.



Data security and industry standards.



Data privacy and data security go hand in hand. A simple way to look at it is that privacy helps establish and maintain data standards and security helps implement and enforce them. At Adobe, we design our products with security in mind. Security is built in early on in the product lifecycle and is an integral part of our initiatives and products.

To keep up with ever-changing standards and regulations, we've created a flexible security and compliance framework that is open sourced. The [Common Controls Framework](#) (CCF) is a set of security activities and compliance controls that provide ongoing compliance across our various products and services. It's the backbone of our security and compliance strategies.

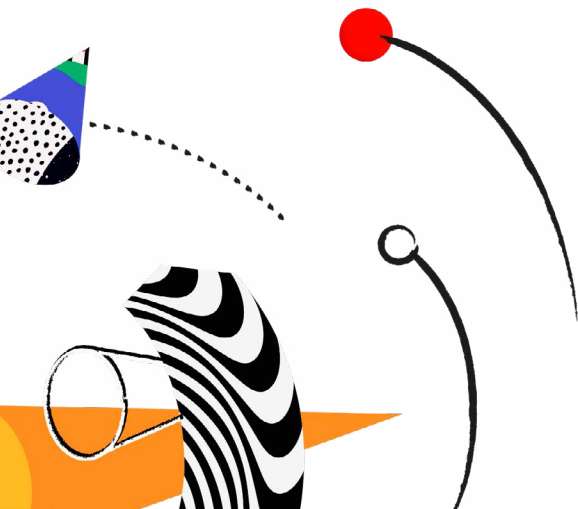
"What worked for us at Adobe – especially in terms of CCF, privacy and security – is we really took a different stance by incorporating security by design," says Rahat Sethi, manager of the technology and risk compliance team at Adobe. "2012 was a good inflection point when we were transitioning into a cloud subscription business. We were already a large company but just getting started on the cloud side. We knew that we had to get ahead of cloud security from the start."

The CCF helps us meet the many certifications, standards and regulations that are essential for data privacy, like SOC 2-Type 2, ISO 27001, FedRAMP, PCI DSS, HIPPA, GLBA, 21CFR and more.

This [complete list](#) includes the completed certifications and attestations we have for each product.

Beyond certifications, we have team members from legal, security and product engineering that participate in and advise many different organisations that influence industry standards and regulations throughout the world. It not only helps us stay apprised of the latest information, but we also get to be part of the discussions. Some organisations and regulatory groups you may want to get involved with include:

- Interactive Advertising Bureau (IAB)
- Interactive Advertising Bureau – Europe (IAB, Europe)
- Digital Advertising Alliance (DAA)
- Digital Analytics Association (DAA)
- Network Advertising Initiative (NAI)
- International Association of Privacy Professionals (IAPP)
- SAFECODE



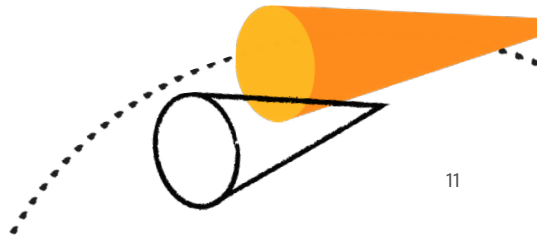
Privacy is a group effort.

Privacy teams need to create open lines of communication with individuals and teams that put data governance policies and procedures into practice. At the top of the list are information security and IT. It's important to make sure each team understands their role and feels a shared responsibility when it comes to privacy.

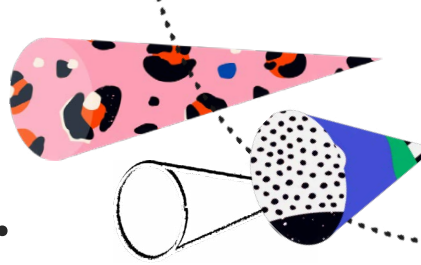
From an organisational standpoint, Adobe has a Chief Privacy Officer, a Chief Security Officer and a Chief Information Officer with teams that work very closely together to stay current on the latest privacy developments around the world and to make sure their technologies are ready to comply. They are solution-oriented partners that also work closely with external audit firms to make sure they're staying on top of what's coming next.

Each team and each individual has unique skills and perspectives that benefit privacy initiatives on all fronts. Consider the strengths of colleagues within each organisation for guidance and precedence. Using technology to address enterprise-wide challenges, for example, is already commonplace for security and IT professionals.

Implementing data privacy is no longer just the responsibility of legal and technology teams. Delivering a positive customer experience is critical across all departments. And as such, an open dialogue is essential to keep all impacted parties involved and informed.



What you can do.



Privacy is personal, on all fronts. What's right for your organisation and your customers may not be right for another organisation. As you embark on your privacy journey, consider these best practices:

- Gather your team of key stakeholders and think through your organisation's business, customer experience, marketing and compliance needs.
- Invest in standardising privacy and security processes early on so that it's baked into your company's DNA and helps make it a positive part of the user experience.
- Review and incorporate industry best practices in ways that work best for your company and stakeholders.
- Think about privacy at the beginning of everything you do and how you can implement for both product and IT infrastructure at your company.
- Create an environment of [co-creation](#) between your IT and marketing departments to ensure the right technology is in place to support positive, personalised customer experiences.
- Continuously research. Read: [Privacy Service Overview](#), [Adobe Compliance Certifications, Standards and Regulations](#), [The Common Controls Framework](#) and [ECID Overview](#).

There are many ways to maintain and achieve privacy and trust with your customers. It's a journey that is constantly evolving. And we're here to help.



Adobe can help.

At Adobe, we're not only committed to giving you the tools you need to bring together customer data from every interaction and channel, we're committed to giving you the flexibility you need to deliver positive consumer experiences that comply with industry and organisational standards. Discover helpful resources and learn more about how we're handling privacy, security and governance at the [Adobe Trust Centre](#).

[Get details](#)

Sources

"Adobe Compliance Certifications, Standards, and Regulations," Adobe, 2020.

"Adobe Experience Platform Overview," Adobe, 9 November 2020.

"Adobe Experience Platform Privacy Service Applications," Adobe, 5 November 2020.

"Adobe Experience Platform Privacy Service Overview," Adobe, 3 November 2020.

"Adobe Experience Cloud Privacy," Adobe, 28 July 2020.

"Adobe Privacy Centre," Adobe, 2020.

"Adobe Trust Centre," Adobe, 2020.

Amy de La Lama, "Privacy Fatigue and How to Combat It," IAPP, 4 January 2021.

"Best Practices for Data Privacy Programs," Ionic.

Clint Eagar, senior technical product manager, personal interview, ObservePoint, October 2020.

"The Common Controls Framework," Adobe, December 2019.

"Customer Journey Analytics Privacy Overview," Adobe, 2 December 2019.

Elizabeth Sexton, senior product manager, personal interview, Adobe Experience Platform, Adobe, October 2020.

Fatemeh Khatibloo, "Make Privacy A Competitive Differentiator," Forrester, 12 November 2020.

Giselle Abramovich, "How CIOs and CMOs Will 'Co-Create' in 2020," Adobe, 18 December 2020.

"Privacy in Real-time CDP," Adobe, 9 November 2020.

Tina Moffett et al, "Forrester Wave": Data Management Platforms, Q2 2019," Forrester, 13 June 2019.



Copyright © 2021 Adobe. All rights reserved.
Adobe and the Adobe logo are either
registered trademarks or trademarks of Adobe
in the United States and/or other countries.