Adobe

The experience privacy paradox.

In a perfect world, brands anticipate what customers want and offer the right experience at the right time. At the same time, customers are more worried than ever about their data privacy. **71%** of European customers are concerned about how companies use their data.

Contrary to popular belief, privacy concerns are not an 'old people' thing. While it is true that about **82%** of baby boomers worry, **77%** of millennials and **73%** of the online-savvy generation Z worry, too. Many customers also speculate about why brands are even collecting customer data. For example, **46%** of European customers believe firms might sell their data. More importantly, only **46%** of Europeans believe that sharing their data is worth the risk. When it comes to data sharing, marketers have yet to make a convincing case with customers. **It's no surprise, brands are increasingly concerned about keeping customer data safe**.

> "It takes time to build trust and you can lose it overnight. We need to do whatever it takes to get the maximum security for our customer data."
>
> **Serge Raffard, Group Strategy and Marketing officer at global insurance firm Allianz**

Allianz

Better personalisation and privacy may sound like competing targets. It doesn't have to be that way. As Adobe's latest research reveals, leading marketers are already providing highly personalized customer experiences, while using customer data responsibly. They make data privacy work for both customers and the company—and act with empathy whenever things go wrong.

Make data privacy work for customers and for the brand.

1. Turn data privacy into a powerful brand benefit.

For decades, firms have built successful brands by addressing pain points their competitors did not dare to tackle.

Brands like Asos and Amazon pioneered free delivery and returns. Unlike its competitors, the US airline Southwest includes a free checked bag. These brands stand out from the competition—customers love them. When it comes to data privacy, the top spot is still up for grabs. To get there, customers don't ask for much. **78%** in Europe simply want the power to decide how firms will use their data. **76%** desire more transparency, and **55%** asked that firms use their data only for what really matters—making the customer experience better.

> "Progressive brands should seek to rebalance the value equation, thinking about how they can use data to create value for the customer, not just about how it can profit their own businesses."
>
> **David Lloyd, EMEA Managing Director at Wunderman Thompson Data**

WUNDERMAN THOMPSON

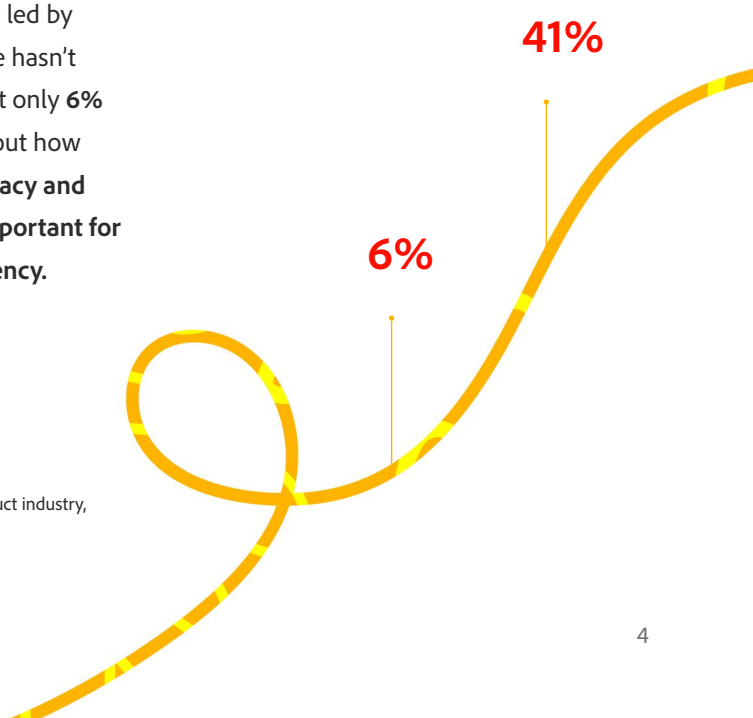
For almost every product category, there is now an opportunity to make the responsible use of customer data a decisive brand benefit. This comes down to being transparent about how their data is used, and giving them real choices, while building experiences that make customers say: 'they really understand me.'

2. Build a culture of respect—starting at the top.

It's hard (if not impossible) for one leader to solve a firm's customer data challenges. Employees at all levels must be involved. Take a simple piece of insight like a customer's age.

This information may sit in one database and then be copied into another. The marketing team uses age to segment for an email campaign. The product team does a subsequent search to understand which products this age group prefers, and so on. Suddenly, this one piece of data was used by hundreds of people. Even if their actions were well intended, the firm could have breached numerous data and privacy laws and, worse, annoyed customers.

Policies matter, but they aren't enough to do the trick. Adherence to data policies and preferences inside firms is typically mixed, according to consulting firm Deloitte.[1] To get data usage right, firms need a much wider approach, led by the company's senior leaders; however, this message hasn't made it into every C-Suite. Adobe's survey found that only **6%** of European executives believe customers worry about how firms used their data. **Only 41% see strong data privacy and governance processes as top priorities. It's now important for senior leaders to treat data privacy with more urgency.**



[1] Building Consumer Trust. Protecting personal data in the consumer product industry, Deloitte University Press.

3. Realise that less data is more.

In the past, marketers have relied heavily on third-party data and simple cookies to target customers. To inform campaigns, many brands are still trying to obtain as much customer data as possible.

Thanks to regulation and advances in technology, third-party cookies and other tracking technologies have been steadily declining and will soon cease to exist altogether. Tracking and targeting across the web will become more difficult, if not impossible. And simply piling up and using masses of customer data increasingly violates privacy laws.

While these changes may sound like limitations they are necessary corrections that will encourage brands to shift away from a conversion at all costs mindset, and toward an approach of building mutually beneficial customer relationships. Leading marketers are now homing in on two data strategies:

A. Building out first-party data.
Instead of relying on data like third-party cookies, leading brands are building their own stores of consent-based first-party data—data that customers agree to share with them. The rationale is simple: The quality of this type of data will almost always be higher—and more effective, and a brand will collect only the data it needs. In many cases, this requires investment in state-of-the art technology. What may sound like a costly investment, however, can net incredible returns in the form of better conversion rates, lower costs and better customer relationships.

B. Asking for less.
To create a personalised experience, marketers often need less—but better—data. One chief marketing officer shared with us: 'I tell my team: every piece of data is an ask from customers.' The moment marketers scrutinise their real data needs, the list of information required often becomes shorter. Asking customers for less data will keep marketers ahead of evolving regulation and also help teams focus.

> "By taking a step back and asking, "why am I collecting this data in the first place?" and approaching data through a customer experience mindset, we encourage a different type of collection, interpretation, and activation."
>
> **Richard Lees, Chief Strategy Officer EMEA at Merkle**

MERKLE

Responsible use of data is the price of admission for earning strong customer relationships.

At Adobe, privacy and security are intentionally and thoughtfully designed into the development of our enterprise tools and services. To contribute to and expand the conversation, we're sharing below how Adobe solutions could fit within your own approach to privacy.

1. 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). 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.

2. Privacy in product development.

Adobe treats 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 Elizabeth Sexton, Senior Product Manager for Adobe Experience Platform, Adobe. "Because they control the data they collect."

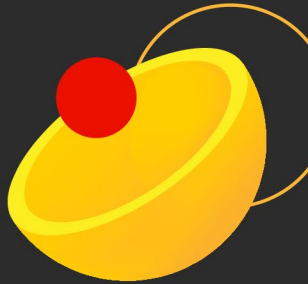
Adobe Experience Platform allows you to unify all your data into robust customer profiles that update in real time. It's the foundation of Adobe Experience Cloud products and helps you deliver the right experience across every channel. It also supports technology and solution partners as they build and 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. **In addition 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.**

3. 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. Adobe, designs products with security in mind. Security is built-in early 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."



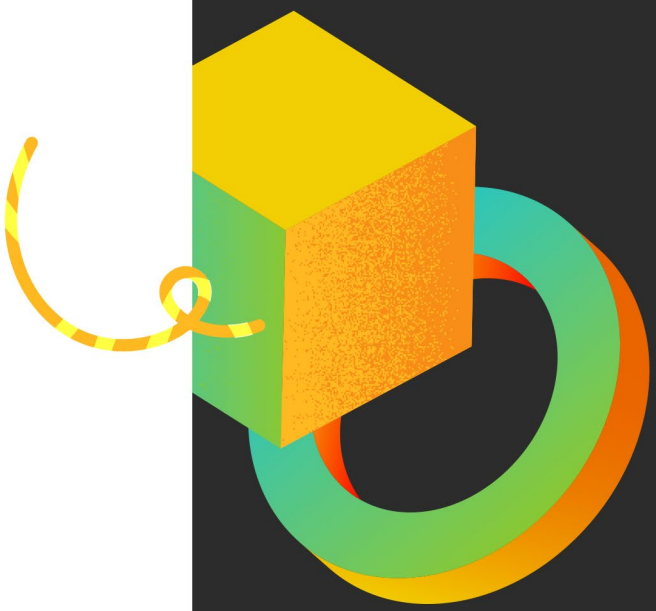
4. Privacy is a group effort.

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.

Each team and 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.

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.



5. Your check list:

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.

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 trusted consumer experiences that comply with industry and organisational standards. Discover helpful resources and learn more about how we're helping brands to deliver transparent, data driven personalised experiences in real time.

Discover more

Sources

1 *"Adobe Compliance Certifications, Standards, and Regulations,"* Adobe, 2021.

2 *"Adobe Experience Platform Overview,"* Adobe, 9 November 2021.

3 *"Adobe Experience Platform Privacy Service Applications,"* Adobe, 5 November 2022.

4 *"Adobe Experience Platform Privacy Service Overview,"* Adobe, 22 October 2021. "Adobe Experience Cloud Privacy," Adobe, 11 August 2021.

5 *"Adobe Privacy Centre,"* Adobe, 2022.

6 *"Adobe Trust Centre,"* Adobe, 2022.

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

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

9 *"Privacy in Real-time CDP,"* Adobe, 9 November 2021.