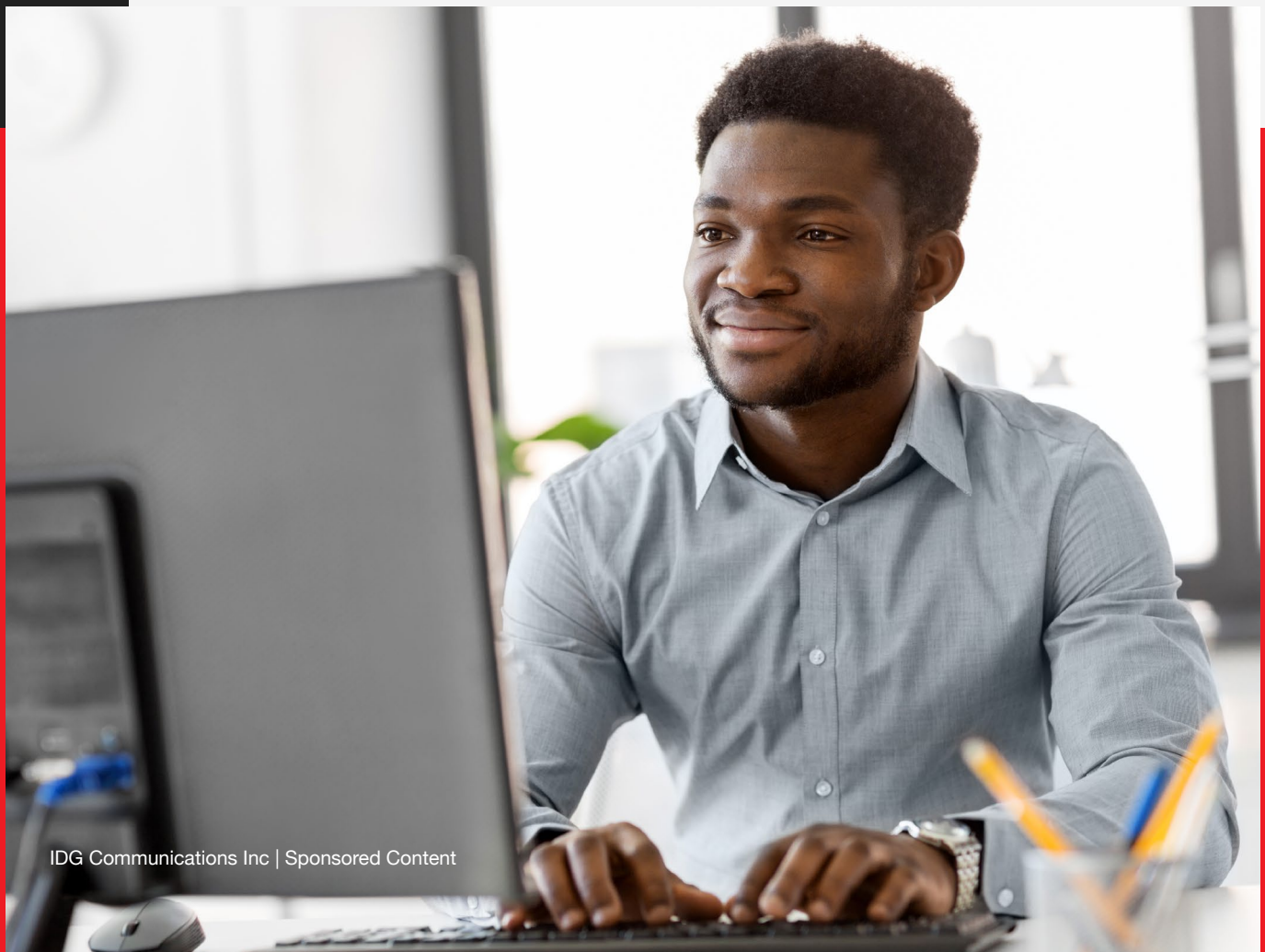
CIO FROM IDG

SPONSORED BY Adobe × Microsoft

Brands that build trust: how data privacy empowers great CX

Businesses need to show consumers that their data is in safe hands

CIO 5M READ TIME



A “grand bargain” provided the impetus behind one of the greatest explosions of innovation in human history: the first 30 years of the world wide web. Implicitly and explicitly, customers have handed over their data in return for free content, personalized marketing offers, a better shopping experience, streamlined transactions, and a faster way of completing administrative tasks.

Increasingly, however, both consumers and corporates recognize that something is not right. Today, consumers worldwide spend $1 million every minute online. But breaches have demonstrated just how easily personal information can be compromised. By one estimate, 37 billion records were exposed by data breaches worldwide during 2020.

This combination of mass market adoption of digitalization and expanding vulnerability isn’t sustainable. In the past, customers didn’t give a second thought about their data, and large organizations often followed suit. Today, however, attitudes are changing in the wake of breaches that have damaged customer relationships and diminished brand equity.

Many consumers have been through a lengthy learning curve. The results become visible in the conflicted responses that emerge whenever they are asked about the grand bargain. Typically, consumers appreciate a better customer experience. They like well-targeted marketing and offers that make sense. But in a recent study undertaken by the professional services firm KPMG, 87% of US consumers said they regard data privacy as a fundamental human right, and 54% do not trust companies to use their personal data in an ethical way.

This is precisely why discussions about data privacy now need to occur in the boardroom: the risk of lagging behind consumer attitudes is real and palpable.

Data privacy the necessary ally of customer experience

According to Adobe's 2021 Digital Trends Report, 92% of marketing, e-commerce, advertising, and creative professionals believe that data privacy is a fundamental part of the customer experience. Yet only 53% of executives at organizations offering customer experiences rated "average" say that privacy and consent is a key factor in their planning.

In more than one way, that's a missed opportunity. Weak privacy strategy is typically linked with negative consequences including sales delays, triggered when customers find themselves needing to know more about how a product or service will capture and exploit their data.

This combination of mass market adoption of digitalization and expanding vulnerability isn't sustainable

The good news is that a successful data privacy strategy doesn't need to blunt the cutting edge of creative digital marketing. In fact, it can serve to enhance competitive advantage, improve investor sentiment, and increase organizational agility.

BMW, for example, has spent much of the past year implementing a plan to replace sales through shuttered showrooms with digital selling. The company aimed to make customers feel as valued on this digital journey as they traditionally would in a car showroom. Underpinning this approach was a state-of-the-art tool stack, high-quality customer insights, and a permanent organizational shift toward collaboration and knowledge-sharing between central and local marketers.

BMW's new global digital marketing platform has been a success in sales terms. But for our purposes, what matters are the project's underpinnings. These support an advanced approach to data privacy that goes hand in hand with increased sales effectiveness.

Any organization hoping to make a similar transition needs to think in terms of five key steps on the journey to remaking the grand bargain between vendors and customers.

- **Identify and classify all datasets**

To meet the minimum benchmark in a privacy-aware age, organizations need to be in control of their data. The starting point for businesses is to identify the locations in which data is kept and classify it so that it can be protected by appropriate controls. (For example, the data in question might be destined for public consumption, or not. It might be non-business data, or classified as confidential.) Old datasets require particular

scrutiny: they frequently need cleaning, deletion, or additional protection. As global brands look for additional insights into their data through machine learning and artificial intelligence, policies around Responsible AI should be implemented, constantly updated, and transparent.

- **Deploy the tools of data management**

The primary requirement is an end to data siloes, replacing them with systems that allow data holdings to function as a single source of truth. The result facilitates a better understanding of customer journeys, leading to a 360-degree customer view, making compliance with data protraction laws more straightforward.

- **Elevate responsibility to board level**

The most visible signal that privacy is taken seriously in any organization involves defining it as a board-level concern. At this level, privacy can hope to become embedded within overall business strategy — and not just online, but in physical outlets, among sales teams, and within the supply chain.

> **They think of data as a strategic asset, rather than as a commodity with attendant costs of compliance**

For customer-facing organizations, in particular, this may mean appointing a chief privacy officer (CPO), who handles compliance and/or incident response, and works closely with an existing chief security officer (CSO/CISO). The organizational structure is less important than the key responsibility, which is to brief the board at regular intervals on the company's data protection posture and associated risks.

· Enforce privacy by design

The EU's GDPR directive incorporates the requirement for organizations to build services and applications that come with data privacy mechanisms embedded. Examples include clear, repeatable processes that help development teams build the necessary protections into systems, as well as networked infrastructure and operational practices. The same logic applies to software acquired on the open market, which needs to comply with your organization's policies.

Recall, too, the contribution that SaaS applications make to privacy by design. Cloud-based applications are constantly updated with little or no interruption to operations. All other things being equal, this makes them more secure than on-prem applications, reducing the risk of data breaches that expose customer records.

· Act like you mean it

Organizations that prioritize data privacy think and behave in specific ways. They think of data as a strategic asset, rather than as a commodity with attendant costs of compliance. Taking advantage of their ability to generate a single view of the customer, they will frequently offer customers a single online location for defining user preferences, including opt ins and opt outs. Acknowledging that customer anxieties are unlikely to be quelled by a cookie consent form on their first visit, they explain to customers what information they collect, and why. And they communicate with customers when their policy changes. (Microsoft, for example, enhances transparency by publishing a change history for its privacy statement, detailing how it has evolved over time.)

Rewriting the grand bargain

Personalized and data-driven customer experiences have become indispensable in the digital economy. Much of this success depends upon continued assent by the customers whose

data underpins these processes. As we've seen, customer-facing organizations can no longer take approval for granted.

The aim must be to build a platform and a culture that allows your organization to transform its compliance efforts into something that visibly contributes to enhanced brand reputation and better customer relationships.

According to Adobe's recent 2021 Digital Trends Report, only 21% of marketers and other customer-facing professionals say their organization is "very effective" at communicating how customer data is collected and used. Fewer still think they get their approach right the first time: only 16% believe they are "very effective" at communicating the value offered in exchange for customers' consent when they first encounter the brand.

The opportunities here are substantial. Implementing a pro-privacy culture, technologies, and processes will prove to be a necessary condition of surviving and thriving as a digital business in the 21st century. To save the grand bargain, business needs to rewrite it — on terms that consumers find acceptable.

Trust is absolutely paramount for CIOs — learn more about why no business can afford to make mistakes with customers' data.

Personalized and data-driven customer experiences have become indispensable in the digital economy