What Is Privacy UX? And Why Do You Need It Now?

How consumer demand for data privacy protection can provide a competitive advantage for enterprises using the right platform.

crownpeak

Contents

Introduction

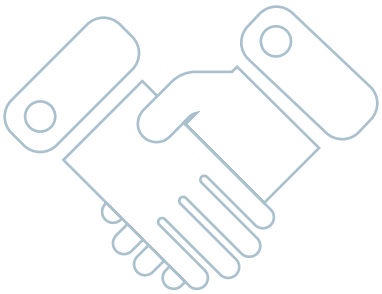
Your compliance team may have already burned a tanker truck's worth of midnight oil while making your enterprise GDPR-ready. But just when you thought you could breathe a sigh of relief, there's the imminent arrival of the California Consumer Privacy Act (CCPA) to prepare for.

But wait: After that, there's the EU's upcoming ePrivacy Regulation. Not to mention the new regulations being separately drafted or already signed into law by *nine U.S. states*, at least one of them (New York's) being even more stringent than the CCPA.

As **Forrester noted** in announcing its June 2019 survey on data privacy statutes in 61 countries:

"Apart from EU's GDPR to California's CCPA and Brazil's LGPD which have been passed, more regulations are in the works, including those from other US states like Massachusetts, as well as India and Japan."

Where does it end? The answer is, it won't. The seemingly sudden arrival of all this new regulation isn't due to some eruption of spontaneous legislation on the part of lawmakers. It's because of consumer (aka constituent) demand. People are now expecting more online privacy protection, and who's to blame them?



Build trust, not just compliance

According to a **PwC study**, a mere 12% of consumers say they trust companies more today than they did last year. High-profile cases like Facebook/Cambridge Analytica may have first prodded their sensitivity around data privacy, but new headlines keep popping up to reinforce their concern, like British Airways being fined $233 million for allowing malware to skim customer credit card data from its websites. In that climate, it's no wonder regulators are looking to clamp down – hard – on data privacy violations.

Yet there is room, even in all this madness, to breathe a sigh of relief. Because there's a vital strategy for coping with this current of change, one that even provides fresh business opportunity. Smart companies won't simply focus on compliance, but on how to capitalize on the root cause of all that regulation. Since the *increase* in data privacy regulation owes to a *decrease* in consumer trust, then finding the right platform for establishing and growing that trust can help build your bottom line.

And as we'll see, Privacy UX is that tool. By combining CCPA, ePrivacy, and GDPR consent requirements in a seamless, engaging user consent experience that aligns with a brand, the bond of trust between consumer and marketer isn't just preserved – it can actually be deepened as never before.

Between January 1, 2005 and July 31, 2019 there were 10,697 recorded data breaches.

ID Theft Resource Center

The privacy movement and business landscape

A worldwide movement

To date, data privacy laws have been enacted in over 80 countries worldwide, many of them bearing a close resemblance to the European Union's General Data Protection Regulation (GDPR). Here are just a few examples:

Argentina

Argentina's Personal Data Protection Act Law of 2000 applies to any individual or business within the country that deals in personal data, a definition that extends to browser cookies. So tracking user behaviors on a website or ad network makes a business liable, under the law. Like the GDPR, personal data can only be handled or processed if the subject has given prior informed consent, and they can request deletion of their data at any time.

Hong Kong

The **Personal Data (Privacy) Ordinance** (PDPO) mandates that a person must be informed of any personal data collection, and who the data may be transferred to (such as if you're using a third-party email marketing service to distribute newsletters). Violations could mean fines up to HK$50,000 and up to two years in prison; plus, violators can be sued by the people whose data they've mishandled.

Mexico

The **Ley Federal de Protección de Datos Personales en Posesión de los Particulares** (LFPDPPP) was enacted in 2010, and is meant to protect individuals' personal data. Unlike the GDPR, though, the LFPDPPP isn't extraterritorial, but the types of data protected by it and the GDPR are similar, so a business operating in Mexico needs to be conscious of how easy it may be to become subject to its provisions.

Philippines

The Philippines are regarded as having **extremely tough data privacy laws**, as anyone gathering personal data needs to obtain specific and informed consent from the user and declare the purpose of the data processing up front (or as soon as possible afterwards). Users have the right to know your identity, what data you're processing and to what end, who you're sharing it with, and what their rights are with regard to that data.

Even countries with strong individual constituent provinces or states, like Canada, have uniform *national* laws. When you turn to the United States, however, it's quite another situation.

The hodge-podge within U.S. borders

As mentioned, the drive toward state-by-state data privacy laws has taken hold well outside of California. Part of the reason? The federal government has, thus far, failed to draft, let alone enact, comprehensive national data privacy legislation of any kind.

The **CCPA** is a tough law, giving consumers new rights in regard to the collection and sharing of their personal data. For companies hoping to conduct business in the fifth-largest economy in the world, being compliant with California's new law, set to go into effect on January 1, 2020, is mandatory. Like the GDPR that came before it, it's a law with teeth: if a person asks you to remove their data from your files and you neglect to do so and are still found noncompliant 30 days after notification, you can be fined $2,500 per individual. If the California courts suspect you held onto that data willfully, they'll triple the penalty.

That's for *one* person, but imagine failing to delete the data of one thousand, ten thousand, or even more from your database. If a company's data handling policies and architecture aren't up to snuff, it's all too possible it'll find itself in a multi-million-dollar CCPA compliance hole.

But like we said: The CCPA is only the first among many emerging state privacy laws. Here are a few of the others, with a few differentiating details called out:

Washington

The Washington Privacy Act failed to pass in this legislative session because the tech sector, legislators, and privacy activists couldn't see eye-to-eye on what it should look like in final form. The proposed law was similar to the GDPR and CCPA in many respects, but even more restrictive on some fronts. Failure to pass this year doesn't mean it won't be signed into law at some point in the future.

Delaware

In 2015, the state passed the Delaware Online Privacy and Protection Act (DOPPA), featuring a range of requirements directed at consumer-facing websites. Those included requiring the conspicuous posting of a privacy policy and prohibiting marketing age-inappropriate material to minors.

New Jersey

What's intriguing – or headache-inducing, perhaps – about the New Jersey law is how its protections are for the "customer" who is "an individual within this state." That's as opposed to the CCPA, which protects a California "resident." The upshot? Even if they're not a resident of New Jersey, a person is protected so long as they're within the boundaries of the state when the data is collected. This bill is still in its nascent stages, and this definition will probably be refined, but it's an example of the potential state-by-state regulatory variations that can have painful implications for corporate compliance teams.

The impact on business

One obvious implication? Companies will have to deploy significant resources to meet the obligations and manage the risks posed by the raft of new regulations. **According to Gartner**, by 2020 *"the backup and archiving of personal data will represent the largest area of privacy risk for 70% of organizations, up from 10% in 2018."*

Organizations that don't revamp their data retention policies will face major risk of sanctions, not to mention the issues that come in the event of an actual data breach. The GDPR, for instance, levies regulatory fines of up 4% of annual global turnover or €20 million, whichever is greater, for noncompliance.

The costs of coping with this profusion of new legislation and the data privacy mandates they impose is significant, but **the costs of noncompliance can be much larger**. If you're caught out violating regulations, or even your own stated policies, the financial penalties and the black eye you suffer in the media can be huge. Uber, for instance, paid $148 million to settle a lawsuit brought by every state Attorney General in the U.S. alleging the company had tried to cover up a 2016 data breach. That was before the imposition of legislation like the CCPA.

In the 12 months after GDPR inception, there were 144,376 data privacy complaints filed and 89,271 data breach notifications.

European Data Protection Board

The risk spectrum

As you start to define your approach to data privacy laws, you'll likely reach a better understanding of the tolerance for risk your organization currently operates under. Heavily regulated industries like financial services and healthcare usually find their legal and compliance teams hold a significant amount of power, resulting in a very *low* risk tolerance.

What we see is that organizations with a low tolerance for risk — such as healthcare — will usually experience a high, and negative, business impact as major data privacy laws come into effect. Anyone that's gone through the process of getting ready for the GDPR by embracing the strictest definition of the law has probably already experienced this.

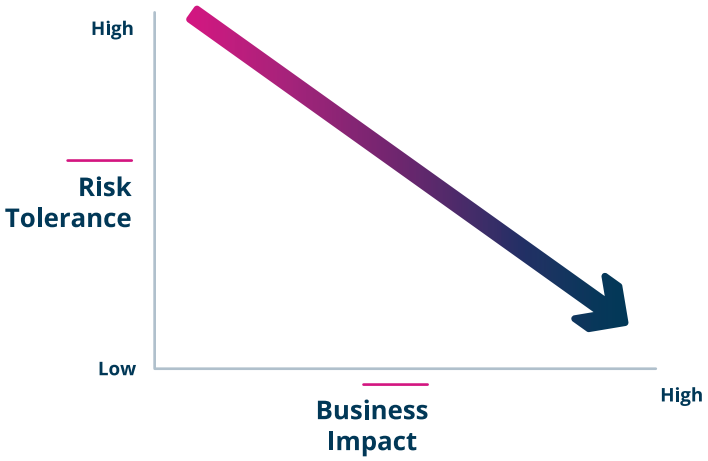
In the first year of GDPR enforcement, the Supervisory Authorities of 11 EEA countries imposed €55,955,871 in GDPR-related fines.

European Data Protection Board

What that means is that laws like the GDPR, CCPA and others can result in a massive disruption to "business as usual," if companies commit to reducing their regulatory exposure.

Here's how the relationship of "risk tolerance" to "business impact" lays out, as it relates to data privacy laws.

What confirms this model? Consider the number of businesses that have either shut down operations entirely or ceased doing business in Europe as a result of GDPR requirements. Of course, neither of those approaches are necessary, or even appropriate, to comply with even the strictest interpretation of the law.



crownpeak

The potential pain of "wait and see"

What's the possible impact of a law like the CCPA on a company that isn't compliant? The fact is, *nobody* should sit on their hands. The GDPR has already furnished many cautionary tales of what can happen to companies that stand pat for too long.

Still, a large portion of the market will take the "high risk, low impact" approach when confronted by new data privacy laws, betting on a lack of regulatory activity. The resultant impact to the business is minimal, but the risk of regulatory sanctions is high. GDPR, CCPA, LGPD, and other similar data privacy laws were *meant* to disrupt data collection practices across the web, so fostering a "business as usual" mentality is a gamble.

Nonetheless, until the regulatory hammer begins to drop and fines and decisions are handed out, this will remain a preferable option for a lot of enterprises. But when regulation begins to bite, you may find your legal and compliance team beginning to reconsider their original stance on regulatory readiness.

Changing your approach will likely force you down the curve towards a lower tolerance of risk. But with that comes a higher likelihood of business impact. For example, perhaps your legal team is now asking you to start getting consent *before* you drop cookies on the user's browser, a situation where you'd previously relied on "implied consent."

This move towards a stricter consent definition will likely result in some friction from your marketing teams, alarmed at the potential loss of valuable customer data and analytics. But your legal and compliance teams are probably aware, even now, that "business as usual" is nearing its expiration date, especially in light of the potential damage your company might have to endure.

Reputational damage

As Gabe Morazan, a certified information privacy professional/Europe (CIPP/E) and Director of Product for Crownpeak's Privacy UX and Consent solutions, has pointed out, "If you take a short-sighted point of view on this, you're swimming against the tide, and you're overlooking the fact this is a consumer movement, not a regulatory issue. So a company may miss out on the real opportunity it presents."

In a marketplace where one of the most important currencies for consumers is *trust*, brands that go the extra mile to earn it will reap reputational benefits that drop straight to the bottom line. But if they fail at protecting consumers' personal data, or mishandle it, they're playing a very dangerous game.

There's varying evidence about whether the reputational damage resulting from regulatory violations or data breaches is truly permanent. Some companies that have seen serious breaches haven't sustained long-term injury, but it's not uncommon for the people manning the executive suite to suddenly find their seats have gotten very hot, indeed. In the case of Equifax, its stock price dove from $147 per share to $90 after the breach, its CEO, CIO and CSO were all shown the door, and Moody's downgraded its credit rating. That ex-CEO later had to occupy another hot seat – testifying in front of Congress.

According to the "State of Cybersecurity: 2019" **report by the ISACA**, most global cybersecurity professionals believe that most companies underreport breaches or other incidents they're required to publicly disclose, not to mention the ones they aren't legally required to make public.

A big contributor to this evasion? The reputational damage they've seen suffered by other companies that have admitted to breaches or mishandling of consumer data. There's also the matter of the legal, IT, and operational costs of ensuring compliance, which they'd rather duck or postpone. These costs aside, the hard dollar penalties involved in noncompliance are extremely real too.

Fines and penalties

In the case of the CCPA, we recounted earlier how a failure to delete a user's data can result in a $2,500 fine per instance, a fine that triples if a court finds you've "deliberately" kept the data. A failure to audit your existing data collection systems and processes, and those of your vendors and third-party partners, is one of the most likely ways to incur such a hit, and one way a "wait-and-see" attitude can translate into bottom-line disaster.

Companies with websites, or multiple websites, where third-party apps are firing tags and gathering data, are putting themselves in grave danger of CCPA violations. Even a year after GDPR implementation, **almost 60% of apps on sites** which fell under its purview were found to be sending consumer IDs to remote endpoints, according to an **AdExchanger study**, "regardless of where the users were located or whether they'd given consent."

British Airways is a prime example of a company allowing others to run exploits on their digital sites. While it was a case of black hat malfeasance, it's still a situation where better oversight might have caught the problem before it escalated into a $233 million migraine.

Inaction isn't an option

Today, company websites and data-handling ecosystems can be so complex, so reliant on third-parties and marketing partnerships, that companies can't afford to sit back and leave protection of their cyber-hygiene to external parties, especially when it comes to the CCPA. Lack of inhouse controls and proper process can leave companies wide open to vulnerabilities in their partners and suppliers.

To gain a firm handle on data privacy compliance and to head off the potential costs and damages we've mentioned, it's time for companies to take a proactive approach to managing their *entire* data privacy ecosystem, by taking the right steps right now.

55% of M&A professionals surveyed said they had worked on deals that fell apart because of concerns about a target company's data protection policies and compliance with GDPR.

Merrill Corp

The rewards of compliance

So, what are the benefits to your organization of taking a proactive approach to data privacy?

Penalty avoidance

This is the most obvious: You'll avoid the potentially ruinous penalties that can arise from noncompliance. We've touched on the GDPR and CCPA penalties, which can escalate into the tens of millions. But beyond the costs, there's the damage these penalties can do to business relationships: An organization that violates regulations may unwittingly drag a partner company into the melee, since they've shared data, and may even be violating contractual agreements with other companies that pertain to privacy protection.

Breach prevention

Most privacy laws speak to the need for data collectors to protect data, and implement strong security measures to prevent breaches. These actions will also help preserve trust, retain customers, and avoid the fines and civil suits that go hand-in-hand with modern data breaches. The direct costs of a data breach are bad enough: A study by IBM and Ponemon revealed that the average cost of a single data breach for organizations worldwide is ***$3.6 million***. But the indirect costs can also be significant – a Ponemon-Centrify study found that **65% of customers involved in a data breach lost confidence in the guilty company,** and a quarter of them took their business elsewhere.

Consumer protection

The damage hackers do to individuals with their pilfered data may pale in comparison to the costs to a corporation, you might think. But it really doesn't, especially when we scale our perspective to consider the damage being done to thousands, or even millions, of people, and the proportionate impact such crimes have on each individual. This is where the other benefit of breach prevention exists: You're helping your customers or consumers avoid the all-too-common pain and harm that can result from criminals obtaining their personal data. Establishing a strong reputation for defending data builds a foundation of trust that drives brand loyalty. A **Bank of America study** revealed how...

"...nearly 40 percent of consumers have had their credit or debit card, bank account or other personal financial information stolen. And 20 percent of those consumers who have had their information stolen said they would not shop with a small business that has experienced a data breach."

Build brand value

Your brand is one of your most important assets, but compliance violations and data breaches can compromise it. A **Forbes Insights report** found that 46% of enterprises that had a privacy breach suffered damage to their reputation and brand value. By clearly taking strides to protect consumer data and demonstrate authentic, transparent, and rigorously-observed data privacy practices, companies have a golden opportunity to elevate their brand above competitors who've either taken that "wait and see" stance, or aren't doing enough to communicate their pursuit of data privacy.

Growth in consumer trust

Pew found it was important for no less than 93% of Americans that they have control over who had access to their personal information, and 90% wanted to control the specific types of information being collected. Organizations that implement the privacy protections demanded by consumers will become preferred; witness how Apple and Amazon have become much-trusted brands by staking out the high ground in defending personal data privacy.

Competitive advantage

According to the **U.S. Census Bureau**, nearly three quarters of U.S. households using the web had worries about online privacy and security in 2017, and a third said they'd avoided online actions because of those concerns. So showing your commitment to digital security and privacy protection can give you a big leg up on competitors who don't display the same level of dedication to consumer needs.

The global cost of cybercrime is expected to exceed $2 trillion in 2019, a four-fold increase versus 2015.

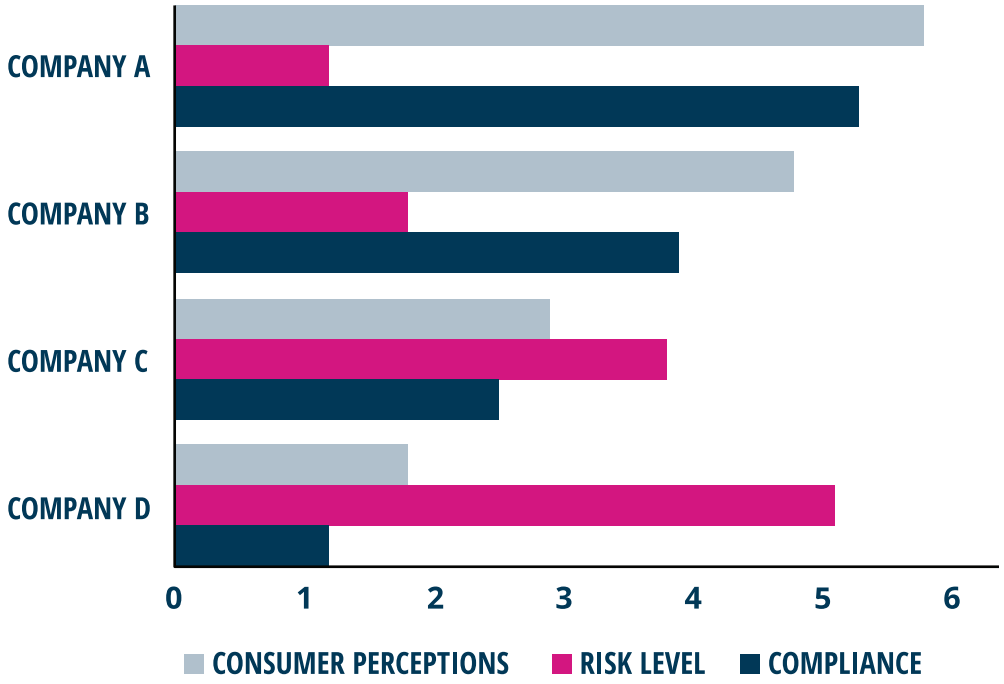
Juniper Networks

Your place in the compliance continuum

Let's picture a "compliance continuum" that indexes the connections between data privacy compliance, risk level, and public perceptions of an enterprise. For two of these, there's an obvious and proven linkage: Lack of compliance drives increased risk of violations, penalties, breaches and other problems.

Connecting these with consumer perception may be more elastic and imprecise right now, but negative examples (Facebook and Equifax) and positive ones (Apple and Amazon) are beginning to show there's a concrete correlation between data privacy protection and consumer sentiment.

Where do you think your company falls on this kind of a continuum?



Are you Company A, whose proactive compliance efforts, transparency, and responsiveness to consumer concerns about data privacy have both reduced risk and increased its standing with its target audience?

Or are you closer to Company D, where a lack of compliance effort will – if not now, in time – drive down those perceptions and eventually hurt your customer retention and market share?

Defining privacy UX

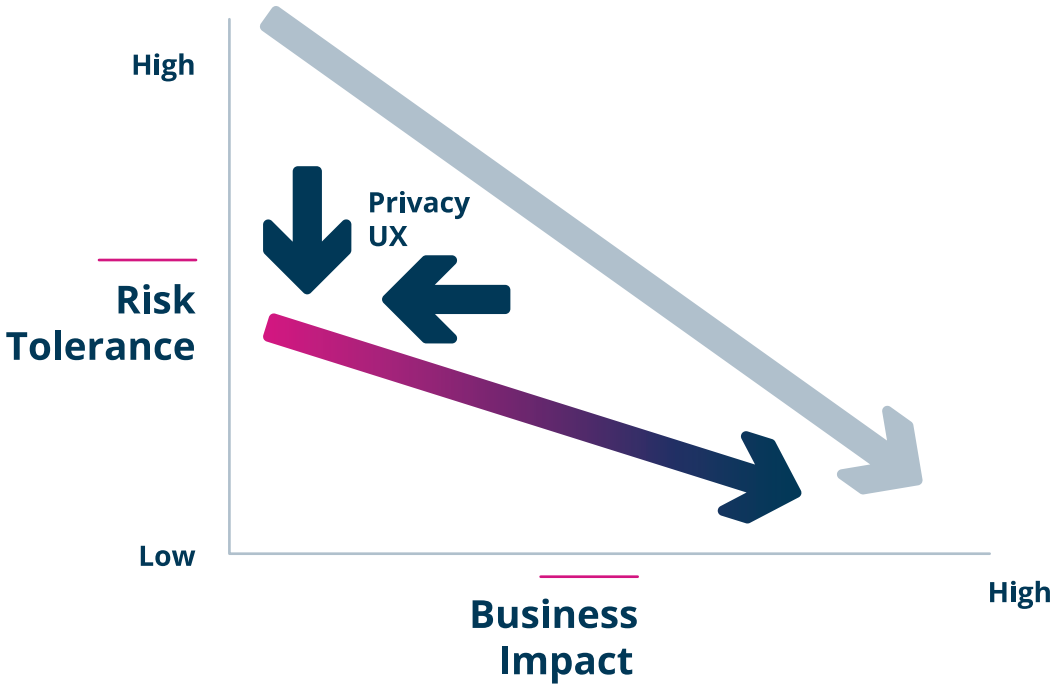
Where should a visitor to your website or other digital property first encounter your commitment to data privacy? Your consent solution provides the first visible signal of your organization's approach to privacy, and can be considered the foundation stone for building customer trust.

By building a "privacy user experience," or Privacy UX, that flows seamlessly throughout your visitors' digital experience, you're proving how embedded your respect for privacy concerns has become. **The right Privacy UX will perfectly match the tone of your site, the persona of your brand, and the messaging architecture and look-and-feel your visitors have come to expect.**

Privacy UX will make your visitors more comfortable with continuing the engagement they've had with you in the past, or that they're experiencing as new visitors or customers. That comfort level makes them more willing to share their personal information with you.

Privacy UX is about taking best practices from the field of user experience and human-centered design and applying them to data collection and privacy interactions. Once you start looking for ways to optimize your opt-ins or reduce the bounce rates that have increased due to your present consent experience, you're already starting to think in Privacy UX terms.

As a business's tolerance for risk shifts towards a more conservative approach, you'll find yourself pressed for ways to minimize the business impact. Privacy UX is one of them.



Privacy UX encourages users to opt in to your marketing initiatives, and increases the value of your data. How does it do it?

By highlighting the value exchange: Research proves consumers are more than willing to share their data or consent to cookies when they trust and value the relationship with the brand and understand the benefit they're getting out of it. If you're not clear in your language or experience about how they're rewarded, expect them to opt out (or never opt in).

By being human: Nothing turns users away like reading the words "we care about your privacy." Why? Because that's what everyone says, including the most egregious violators of data privacy rights on the web. It's a meaningless phrase, and certainly doesn't sound like something your brand would say, so why say it? Review the copy and text you're presenting in your consent experience and privacy policy and ensure that they're forthright and sincere, and project authenticity that aligns with your brand. People will trust it, and the relationship you're striving to establish, if content sounds like it's coming from a fellow human being, and represents true values.

By staying on brand: Just like "be human," your users can tell the difference between an experience designed by your branding agency and one designed by your privacy officer. If you're looking for users to opt in, they have to trust you've taken the time to explain and outline the exchange of data collection in a way that matches your brand design. Your marketing team likely frets over every pixel and font on your site, always trying to present the best experience possible. Then you drop an unsightly, mismatched, stiffly-worded consent banner at the bottom of your home page? Show them you've designed and written an opt-in journey that's on par with your brand design, and they'll be more receptive to giving consent.

By using privacy as a point of difference: Apple is using privacy as a way to differentiate itself from its competition, capitalizing on consumers' loss of faith in the tech space and recognizing the value of creating trustworthy experiences for them. Expect others to follow suit as more focus is given to all
mistrust and senti
collection. There's no reason you can't do the same with an effective Privacy UX.

Microsoft claimed to have 1,600 engineers working on GDPR compliance.

Microsoft

A platform approach to privacy

One of the challenges for a marketer with a multi-channel digital presence, is how to extend their Privacy UX consistently and concurrently across all points of contact with consumers. Particularly since the marketer will have to navigate the regional, national, and state-by-state patchwork of data privacy regulations we've already discussed.

The solution for any global or multinational marketer has to be a **unified platform**. As the number of digital touchpoints continues to grow, and regulations multiply, organizations need the ability to centrally govern their Privacy UX while still having the agility to customize it to local regulations.

Another benefit of a platform approach? Simplicity. For marketers, a streamlined, single-source platform is far more efficient, stable, and easy to manage than a multi-vendor configuration.

A privacy UX solution 8-point checklist

Adopting Privacy UX starts with finding the right compliance management software to meet your needs. Here are the requirements any potential platform should be able to meet if it's going to deliver the seamless and scalable operability necessary to addressing the challenges we've outlined:

1. Improves your Privacy User Experience by seamlessly integrating it into the overall customer experience

2. Combines CCPA, ePrivacy, and GDPR consent requirements in a single user experience

3. Deploys notices and experiences that vary based on the user's location through a single JavaScript tag, even across digital channels

4. Provides your site visitors with in-depth insight into your third-party vendors, creating transparency and trust between you and your customers

5. Deploys through your existing tag manager and manages which cookies and tags can fire before or after consent to comply with European data privacy laws like the ePrivacy Directive and GDPR

6. Provides a simple form for a user to exercise their rights and request access to their information, as required by the CCPA and GDPR

7. Supports unique and engaging consent experiences that match your brand via robust APIs and partners

8. Has the flexibility and granularity to be seamless incorporated into user experiences across multiple channels.

About Crownpeak

Crownpeak, the only true cloud-native digital experience platform, offers a suite of powerful tools that deliver the industry's fastest time-to-market across web content management, optimization, governance, and privacy UX. Crownpeak helps brands quickly create and deliver digital experiences that build trust and maximize customer lifetime value. On top of its powerful CMS, Crownpeak includes built-in personalization and testing tools, on-site tag and performance monitoring, and content governance.

As the leader in customizable privacy experiences compliant with global privacy regulations — such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) — Crownpeak provides the world's only API-based consent-as-a-service system, able to optimize progressive consent across all devices and channels. Hundreds of Global 2000 customers – including Toyota, Healthgrades, and Unilever — rely on Crownpeak to deliver privacy-first and high-quality digital experiences with a quicker time to market.

Interested in learning how Crownpeak can get you started with Privacy UX? Visit **crownpeak.com/demo-request** to request a demo today.