Report: US and UK Executives Grapple with Evolving Data Privacy Laws

As global data privacy compliance increases in scope and complexity, only about half of executives feel "very prepared" to meet regulatory requirements in the United States, United Kingdom, and European Union.

That is one of the key findings in Womble Bond Dickinson's 2023 Global Data Privacy Law Survey Report, which draws on responses from more than 200 executives in the U.K. and the U.S., nearly half of whom are C-suite executives. The second annual report analyzes the rapidly changing data privacy landscape — including new regulations and the application of artificial intelligence (AI) and other emerging technologies — as well as corporate readiness and the differences between those operating in the U.S., U.K., and EU.

UK outpaces the US in corporate preparedness, but challenges persist on both sides of the Atlantic

As several U.S. state data privacy laws near or reach effective dates, executives with operations in the U.S. are less confident in their preparedness than in last year's survey: only 45% say they are very prepared to comply with U.S. laws and regulations, compared with 59% in last year's survey. With a more established General Data Protection Regulation (GDPR) in Europe and the Data Protection Act 2018 (DPA) in the U.K., more respondents with operations on the continent feel prepared to meet these requirements. However,

these respondents still feel the impact of an increasingly complex regulatory environment, with just 53% saying they are "very prepared" for compliance.

"Europe has long been ahead of the U.S. when it comes to data privacy laws, having had one in effect since 1995, along with the GDPR, which was adopted in 2016," said Andrew Kimble, a U.K.-based partner who focuses in data protection and privacy. "Given all the steps companies need to take, employees at all levels of the organization in the U.K. tend to be aware of the GDPR and DPA."

Yet even confident executives may not be as prepared for compliance as they think. While more than half of respondents have completed such key data privacy measures as designating an internal project manager or owner (70%) and conducting regular training (58%), only 34% have conducted data mapping and understand data practices across the organization.

"Data mapping — knowing what data you have and where it lives — is foundational for any effective data privacy and cybersecurity strategy," said Tara Cho, partner and U.S. chair of the firm's Privacy and Cybersecurity Team. Additionally, while many companies might implement external-facing actions, such as putting a cookie banner on their website or updating privacy policies, Cho notes that there is still a "need to build out back-end requirements to truly operationalize the compliance requirements."

Roadblocks crop up in other areas as well. For instance, half of the respondents doing business in Europe say understanding the data held within their organizations is a challenge, while 45% cite difficulties increasing their budgets. In the U.S., nearly 60% of executives view tracking the status of legislation and the differences between state laws as a challenge, yet only 42% have completed comparisons of state privacy law frameworks.

Cross-border data transfers and cybersecurity are top of mind

In an increasingly global and digital business landscape, the ability to transfer data across borders is paramount. Despite the current regulatory uncertainty in this area, the survey data suggests that data privacy regulations can be helpful for cross-border business — especially for U.K. respondents, who are more experienced with existing standards. Forty percent of U.K. respondents (versus 35% in the U.S.) say these regulations add extra costs but are manageable, while only 10% in the U.K. (compared with 17% in the U.S.) believe regulations are a major impediment to such business.

"While cross-border data transfers remain a challenge, the findings demonstrate that many businesses are managing and even seeing value in associated regulations," added Andrew Parsons, a U.K.-based partner who focuses on commercial disputes around information rights, privacy, and other technology-related issues. "Though much remains in flux, if and when these rules stabilize, they can have a positive long-term impact."

When it comes to big-picture concerns around data privacy, data breaches and cybersecurity rank as the top issue (particularly among U.K. respondents). Litigation and enforcement action ranked second among U.S. respondents.

Growing adoption of biometrics, geolocation, and AI brings new opportunities — and concerns

Most respondents say their organizations use fingerprints, facial recognition, and other biometric data, including 59% of U.K. respondents and 64% in the U.S. (the latter is a five percent jump from the 2022 survey). Amid expanding use, the compliance risks have also grown with biometric privacy laws and several lawsuits in the U.S.

Regarding geolocation data, 40% of U.S. respondents (and 32% of those in the U.K.) are very concerned about privacy laws that include specific restrictions on collecting and using geolocation data for targeted marketing purposes.

The survey also finds respondents accelerating their adoption of AI technologies. More than 1 in 5 respondents (22%) started using such technology in the past year alone, and only 19% aren't using it at all. Respondents cite a wide range of uses for AI, with 36% using the technology to generate content and another 24% planning to do so in the next year. However, respondents cite ethical concerns (45%) and legal risks (34%) as key obstacles to AI adoption.

"Whether it's evaluating loan applications, filtering qualified candidates for a new job posting, or any number of other use cases, AI tools make complex decisions all the time," said Ted Claypoole, a partner who leads the firm's U.S.-based IP Transactions Team. "That's what they're there for. The question is, are they doing it in a way that's improper from a societal and legal standpoint?"

The survey was completed by 205 business leaders in April and May 2023. Respondents represent 22 industries and play either a leading or supporting role in data privacy issues. Half of these respondents (51%) are U.S.-based and represent 33 states. Forty-seven percent of respondents were based in the U.K. Nearly half of the organizations surveyed stated they have offices in the EU, with 25 countries selected. To read the complete report and methodology, please click here.