

As Corporate Legal Teams Prepare for the EU's Artificial Intelligence Act, Partner Keith Enright Discusses the Benefits of Leveraging Established Frameworks with Bloomberg Law

In the Media | April 7, 2025

Bloomberg Law

Europe's Landmark Privacy Law Gives Companies a Playbook for AI

Bloomberg Law

By Cassandra Coyer

April 7, 2025

As EU AI Act provisions come into force, many corporate legal teams have chosen to lean into compliance regimes already tested by another EU law: the General Data Protection Regulation.

The two measures share a common core—including risk assessments, a focus on fundamental rights, and data governance—that has allowed many companies to prepare for the world's first comprehensive AI regulation without having to overhaul their existing processes or deploy significant additional resources.

"The competencies and capabilities that companies developed to demonstrate compliance with the GDPR gave them many of the tools that they needed to demonstrate compliance with new and incremental legal obligations," said Keith Enright, co-chair of Gibson Dunn's AI practice group and Google's former chief privacy officer.

"This will be true of the AI Act over time as well," he added.

But while GDPR lessons can avoid duplicative work, they won't get companies to the finish line. The AI law's scope is much broader and requires companies to be more agile as technology evolves.

A sprawling supply-chain of developers, providers, and users, and questions about where responsibilities will fall, also presents new and complex challenges.

"Managing the third-party topic with GDPR was probably a challenge in itself," said Francesco Marzoni, global chief data and analytics officer at Ikea Retail (Ingka Group). "Now it's even bigger because, again, it's not just a one-off effort—AI models evolve."

By-Design Approach

The EU's 2018 privacy regulation stressed a key principle that has since informed data protection laws and approaches in the US: privacy by design. That principle requires teams to implement data protections at the creation of a new product or technology, instead of after the fact.

The EU AI Act also requires principles of data minimization and protection to be implemented "by design and by default" when

personal data is processed by an AI system. Even when a system doesn't ingest or give out personal details, the act pushes for responsible AI practices from the onset of a product's lifecycle.

"The AI Act says, yes, it's product safety, but it's also fundamental rights," said Jean-Marc Leclerc, director of EU affairs at IBM.

"And it doesn't matter if it's personal data, non-personal data. The requirements of data governance apply to any data."

The European Commission intended for the two laws to complement each other, he added.

Companies have tapped teams responsible for GDPR compliance to apply those earlier lessons to AI regulation.

"It makes sense, because there's a lot of common ground," said Jean-Rémi de Maistre, co-founder and CEO of AI-powered legal search platform Jus Mundi, noting that these teams include AI, privacy, and cybersecurity capabilities. This approach allowed his organization to get ready early on without feeling like it was costing them much more.

Jus Mundi, alongside Ikea and IBM, were among other early signatories to the EU AI Pact, a pledge by nearly 200 businesses to start applying the principles ahead of the AI law taking effect.

The cross-functionality approach to GDPR compliance will be key under the AI law to avoid duplicative efforts.

"I personally don't believe in divide and conquer," said Alesya Nasimova, global head of privacy and data protection officer at Brex. Nasimova said her insights don't represent the views of her employers.

"Let's say you have a data privacy impact assessment for GDPR, and then you need a conformity test for the EU AI Act. You figure out where those overlaps are and create something that's conjoined, instead of having two different assessments," she added.

The Right Benchmark?

Still, some companies that do fall under the AI law's scope—such as startups with cutting-edge use cases or those that don't handle personal data—haven't yet had to comply with GDPR requirements. Determining their approach to AI governance may prove more challenging.

"You'd have to start from scratch for GDPR to even meet the requirements of the EU AI Act," Nasimova said. "So it becomes kind of a double-whammy for a lot of organizations."

Though GDPR serves as a helpful stepping stone, it might not be the perfect benchmark for some of the new challenges posed by the AI law, governance professionals warn. The technology-agnostic aspect of GDPR, for instance, is distinct from the AI law's granular breakdown of AI systems and use cases.

"Use cases really matter in AI, and I'm not sure that appreciation existed with previous technologies and previous regulatory regimes," said Jace Johnson, vice president of global public policy and ethical innovation at Adobe Inc.

Assessing an AI model's robustness as the technology evolves will require spreading responsibilities across an organization instead of relying on one centralized team.

"You need an internal regime that can sit down and review quickly without impeding innovation," Johnson said. "What are the risks at play here? Are they different? Are they similar?"

GDPR's 'Warning'

A lack of clarity about who among different AI stakeholders will be liable for harmful systems also requires legal teams to adapt their processes and tackle procurement contracts more creatively.

The lines distinguishing responsibilities for providers (who make AI systems or models) and deployers (who use already-built AI systems) can be blurry. Companies that buy AI systems but end up substantially modifying them, for example, could find themselves wearing different hats.

That's when the comparison with GDPR isn't always pertinent, IBM's Leclerc said, since "there are so many more actors in the AI

chain.”

As with GDPR, each of the EU's 27 member states will be responsible for enforcement. The European Commission also created a new AI office to supervise the member states' application of the law.

“There's a before and after GDPR, not just in Europe, but globally. It had such an impact,” Leclerc said. “Companies that want to sell an AI, deploy an AI system in the EU, GDPR is a bit of a warning—it sets a precedent.”

Reproduced with permission. April 7, 2025, Bloomberg Industry Group 800-372-1033 <https://www.bloombergindustry.com>

Related Capabilities

[Artificial Intelligence](#)