Tech Change Drives New Legal Strategies

June 2018

Bloomberg Law

Big Law Business

Critical Wrinkles of the New European Privacy Law

AI Strategy Needs Close Watching for GDPR Compliance

By Lisa Singh

Though the EU's first big data privacy law in 23 years is now in force, there's little consensus on the General Data Protection Regulation. Data experts say GDPR—whose 99 articles govern an individual's right to privacy and ultimate ownership of personal data—is the most complex regulation the EU has ever produced.

The law's brevity may contribute to the lack of consensus. The language of its slim 87 pages leaves a lot of room for interpretation.

This includes both the definition of personal data and a special emphasis where artificial intelligence is concerned. GDPR requires the subject's consent for any evaluation of personal information done solely through the use of AI.

GDPR requires consent for any evaluation of personal data solely through AI.

AI 'Black Box' Versus GDPR Transparency

"There is, on the surface, an inherent tension between the transparency requirements of the GDPR and AI," said industry expert Paul Gettmann.

GDPR gives individuals the right to insist that any AI-driven decision—say, on a job evaluation or loan application—be backstopped with human review. That potentially runs counter to what experts call AI's "many opaque and complex decision algorithms" and its "black box" reputation, Gettmann said.

By contrast, GDPR requires that data processing be purpose-specific, and that "automated decision-making, including profiling" based on personal data include "meaningful information about the logic involved." That means people will have to be involved. That means people will have to be involved to review use of AI in decision-making.

Yet the essence of AI's power makes this "right of explanation" a challenge.

AI systems' "inherent complexity gives them high flexibility and learning power, [but] also makes it a challenge to interpret the models—or explain the results—produced by them," said Justin Antonipillai, the former acting undersecretary at the Commerce Department who previously helped negotiate the EU-U.S. Privacy Shield.

Data experts differ on whom the GDPR even covers: EU residents, of course, but a U.S. tourist sharing personal data with an AI-driven hotel site in the EU? Prevailing legal opinion says both.

"The GDPR very specifically does not say 'citizen' or 'resident' anywhere" in the 99 articles, said Anne Mitchell, a GDPR compliance attorney. "It says only and repeatedly, 'in the Union.'"

Steep Penalties for Noncompliance

The regulation's expansiveness will challenge businesses to stay clear of penalties for noncompliance: 20 million euros or 4 percent of global annual revenue, whichever is higher. Not all companies are prepared.

"Many U.S. companies without an EU presence but whose websites target EU-based buyers are being caught by surprise that the GDPR expressly considers them within its scope," said Kimberly Verska, a law firm partner and chief information officer who specializes in data privacy and compliance.

Companies, such as HR firms using automated screening for resume submissions, will struggle to "implement consent, human-based review, and regulatory audits where their algorithms and log files are examined for impact on the rights of data subjects," Verska said.

The same holds for companies in health and finance with "aggressive marketing analytics," said Antonipillai, the former Commerce official who's since founded a privacy and security software company.

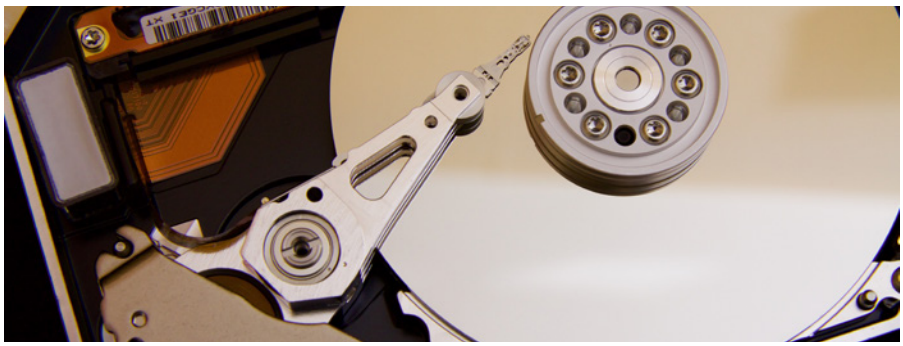
Staying on the Good Side of GDPR Regulators

Companies that demonstrate good faith in compliance will be well received by regulators—at least initially, experts said.

Verska said that will change as regulators obtain more funding and enforcement resources. Officials have already expressed their willingness to "go after anyone, anywhere," said Mitchell, the compliance attorney.

The GDPR includes a private right of action, allowing individuals to file their own grievances—as Austrian privacy advocate Max Schrems did on GDPR's first day, with an $8.8 billion lawsuit against Google and Facebook.

It will be essential to build transparency into AI systems, experts said. "U.S. businesses that leverage AI-driven technologies for data must be much more transparent about their use, and in some cases must obtain explicit consent before their use," said Bret Cohen, a data and privacy lawyer.



It will be essential to build transparency into AI systems.

Experts also stress the importance of hiring a data privacy officer, although, so far, GDPR mandates this only for companies that process personal data on a "large scale," a term left undefined. In similarly nebulous language, a data protection impact assessment is only required when a technology might trigger "high risk," a category that includes profiling, automated decision-making, and sensitive data collection, Antonipillai said.

Keeping Pace with Unfolding Interpretation

It's not yet clear how and by whom GDPR will be interpreted. The Article 29 Working Party, an EU advisory body that is one of the main groups deciphering the law, has issued guidance on AI-like technologies.

"There are many, however, who disagree about those interpretations, and ultimately, just like here in the U.S., the courts are going to make the final decision," Antonipillai said. "The gold standard is always the courts—the European Court of Justice [and] European Court of Human Rights. The European Commission has real depth on these issues."

The application of GDPR's requirements may ultimately extend beyond the EU, and may be driven by consumer demand rather than government action. There's evidence that some companies are anticipating this. As Facebook's Mark Zuckerberg told reporters in April, "We intend to make all the same controls and settings available everywhere, not just in Europe."

Legal professionals can be expected to play a crucial role in future AI-driven technologies, which will mean incorporating the GDPR privacy mandate by design.

Lawyers "can help the tech industry understand their responsibility when designing systems," said Christopher Byrne, chief executive officer of an EU-based email marketing service. "It's never been more relevant than it is today for GDPR—privacy by design should be on every tech whiteboard."

Lisa Singh is a writer specializing in business and technology matters.

Bloomberg Law®

Big Law Business