AI insight into contracts can help ensure GDPR compliance

By Genevieve D. Dong

Businesses across the world are bracing for the impact of the new European Union data-protection regulation, known as the GDPR, which comes into effect on May 25. We in the legal profession are obliged to not only be aware of what's going on with the GDPR, but also to understand what it means to get into compliance.
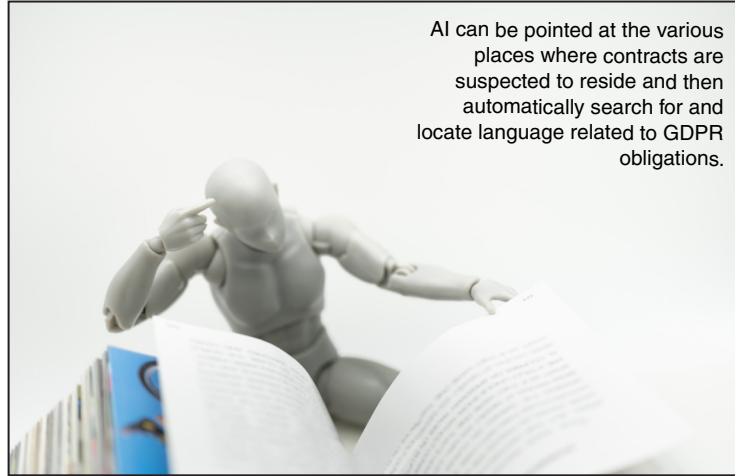
American companies, particularly tech companies, have too often in the past buried their heads in the sand when there were obvious incentives to better safeguard and manage data privacy. You need look no further than the daily news headlines for confirmation.

While the alarm has been raised about America's slow response to this impending mandate, a pervasive lack of understanding of its implications persists. A recent study by Thales revealed that 53 percent of U.S. businesses believe that Europe's new regulations have no effect on their operations.

It is not necessary to be a multinational with operations overseas to fall under the new EU data-privacy regime. Any organization with an online presence that is accessible to Europeans, such as a website, or which uses data from consumers residing in any of the EU's 28 member countries, now faces an unprecedented level of scrutiny both for itself and its third-party contractors.

For those that fail to meet strict compliance standards, the EU has prescribed harsh financial penalties up to 4 percent of the worldwide annual revenue or 20 million euros, whichever is greater.

While the GDPR speaks to a challenging spectrum of data protection and privacy activities, the legal implications also are far reaching. Businesses that lack clarity into contracts often stumble when handling matters of regulatory compliance. This is no less true when it comes to the GDPR, and perhaps even more so.

To be "compliant," a company must ensure that its contracts address a series of specific requirements such as data-transfer restrictions and notice obligations in a data breach event. For example, subcontracting of data processing is a specific concern under the GDPR, and agreements with data processors, or other third parties that may come into contact personal data, must also be reviewed for clauses that define their scope.

To be GDPR-ready, a business must significantly expand its insights into its contracts to correspond with both the direct requirements and the indirect implications of the GDPR. The EU regulations, for instance, directly require a Data Protection Impact Assessment for certain types of data processing. Although not necessarily required, by implication, a well-written contract should also define the frequency of assessments and whether they must be conducted by an independent party.

Considering the topics that must be brought into alignment with the GDPR, from indemnification and force majeure, to termination of rights and limitation of liability, for many companies hundreds of thousands of contracts, often scattered across different locations and departments, will all need to be analyzed for GDPR-relevant clauses.

In the real world, however, resources are limited and the only realistic way to address GDPR requirements is with technology. Compliance cannot rely on a costly manual analysis of each and every contract in an effort to spot factual and contextual issues which may need remediation. This would require armies of legal clerks, and take weeks or even months of man-hours to achieve.

Artificial intelligence technologies can help ensure risks are identified and minimized. AI is already impacting many aspects of the legal profession. With its ability to analyze words and even sentiment and inference, AI can be pointed at the various places where contracts are suspected to reside and then automatically search for and locate language related to GDPR obligations.

AI can be pointed at the various places where contracts are suspected to reside and then automatically search for and locate language related to GDPR obligations.

Shutterstock

Certain advanced contract analysis platforms can employ a type of AI called "machine learning" that uses historical data to get started, then continually improves its accuracy by learning from the human decisions of its users. In a granular sense, this maps the analytics to the specific GDPR regulations.

This process of classifying information that is within the scope of the EU data-privacy rules, and applying appropriate policies to that information such as clauses on when and how to redact, delete, quarantine, encrypt or notify, exposes areas of noncompliance and other potential vulnerabilities.

It's this capacity to accurately assess and forecast risk that is vital under the new GDPR rules, and while also lending itself well to growing regulatory complexity, it gives even greater credence to AI as a potent compliance tool.

Genevieve D. Dong *is a director on the Legal Solution Consultants Team at Seal Software where she engages with legal industry partners to create technology solutions that meet the complex contractual needs of Fortune 1000 organizations. She also serves as counsel at Seal Software, reporting to the general counsel and assists with internal GDPR preparedness within Seal.*

DONG