

CEP Magazine – April 2022

Improving data visibility in third-party contracts with artificial intelligence

By Ceschino Brooks de Vita

Ceschino Brooks de Vita (ceschino.brooksdevita@evisort.com) is head of content marketing for Evisort in San Francisco, California, USA.



**Ceschino Brooks
de Vita**

Compliance and ethics are gaining momentum in the corporate world, with employers creating roles and building teams dedicated to addressing emerging issues ranging from data privacy to diversity, equity, and inclusion. That shift is partly the result of an ongoing movement to promote sustainability and ethical business practices, and partly a reaction to a rapidly shifting business landscape in which consumers and employees—particularly among younger generations—increasingly demand that businesses place as much emphasis on concerns such as environmental sustainability and employee health as they do on quarterly profits. As a practical consequence, this increased scrutiny from all sides entails more work for compliance and ethics professionals in the business world.

While it might not seem like the obvious place to start, a vital area of focus for compliance professionals needs to be contract management and analytics. Why? Because every transaction in the business world, whether it's a customer entrusting their personal data to the business or an employee completing the hiring and onboarding processes, is codified in a contract. As a result, a business's contracts constitute a key data repository for compliance professionals. The promises that a business makes to its customers, or that an employer makes to its employees, are contained in contracts.

Accordingly, it's important for compliance professionals to have ready access to the data contained in the business's contract portfolio. However, it's not enough to simply have access to the documents themselves. Even a small business can easily have thousands of active agreements in place at any given time. As a business scales up and adds customers, employees, and vendors, manually keeping track of the information contained throughout those contracts quickly becomes untenable. Nonetheless, ignorance is not an option. Noncompliance with new regulatory and ethical standards puts the business's reputation at risk and can also result in hefty fines, settlements, and court judgments that are already costing businesses hundreds of millions of dollars.

So what's the solution? Artificial intelligence (AI).

The many uses of AI

What most people are referring to when they talk about AI is machine learning. Machine learning algorithms can synthesize massive collections of data in a fraction of the time it would take a team of humans to do so. They are able to do this thanks to two central capabilities: deep learning and active learning.

Deep learning refers to the scale at which algorithms can operate. Given the infinitesimal amount of time it takes for an AI algorithm to process one data point, AI can process exponentially more data in any given period of time than a person or even a large team of people. Active learning refers to the algorithm's ability to keep improving after it's been deployed. Machine learning algorithms don't need constant training from human handlers to

augment their performance. Instead, active learning enables AI to keep taking new information into account, continuously improving its own ability to parse data.

Natural language processing (NLP) is the application of machine learning to written language, enabling AI to understand the context of words and phrases. NLP helps AI to determine the relevance of a piece of text to a given inquiry. Instead of just matching words and synonyms, the NLP algorithm can consider the author's actual meaning. For example, when reviewing a passage that references defining traits of dogs without ever using the word "dog," a good NLP algorithm that has already been exposed to descriptions of dogs could take those indicators (e.g., tail, paws, domestic, fur) and recognize that, together, they constitute a description of a dog (or at least a household pet, depending on the level of detail in the text).

Contextual analysis also enables AI to determine what's different or missing. For instance, if the passage clearly indicates that the animal in question is feral and has never been domesticated, today's AI would indicate that the animal, while physically similar to a dog, is likely to be something else.

Advances in machine learning and natural language processing have resulted in AI that can effectively read and categorize thousands of documents during the time that it would take a human to read just one. In addition to being fast, AI is more accurate than people. In a study that pitted a team using AI against a team performing manual document review, human lawyers failed to correctly identify up to 75% of relevant documents, while the team using AI needed to review only 1.9% of documents for accuracy.^[1] This is true outside of law and compliance as well: AI is more consistent than humans when it comes to making decisions, such as how to label documents.^[2]

For a compliance professional who needs quick access to compliance terms located throughout a business's contracts, being able to leverage AI that's been trained on contracts significantly reduces the time constraints and operational bottlenecks associated with manual review. Here's a look at two ways a compliance and ethics team can leverage AI to unlock the data stored in their business's contracts.

AI and data privacy

One of the most pressing compliance concerns for businesses throughout a range of industries right now is the evolving field of data privacy. The number and the impact of data breaches have both expanded in recent years as more commerce moves online, with businesses collecting and storing customer data so they can provide targeted advertisements and personalized shopping experiences.^[3] Myriad data privacy regulations have emerged in response throughout a plethora of jurisdictions, all structured to protect the private information that consumers entrust to businesses. More than three quarters of countries around the world have active data privacy laws, and nearly half of those enacted them in just the last decade.

However, ubiquity does not entail uniformity, and compliance with one set of regulations does not guarantee compliance with any other, given their divergent standards. While the General Data Protection Regulation is well established in the European Union, other countries, including the post-Brexit United Kingdom and the United States, are still developing their own regulatory frameworks.^[4] In the absence of a federal standard in the United States, individual states are forging ahead with their own data privacy statutes. The California Consumer Privacy Act is the most prominent, containing provisions that delineate consumer rights and business obligations regarding mandated risk assessments and timely notification of data breaches. However, even that standard is set to be subsumed by the California Privacy Rights Act, which will amend and expand the California Consumer Privacy Act effective January 1, 2023.

Compliance officers must also contend with different standards for different types of data, as a number of

jurisdictions have passed or are actively considering separate laws protecting biometric data: physiological or behavioral identifiers including a person's face, irises, fingerprints, voice, hands, and handwriting.^[5] In the US, legislation to protect biometric data is currently under consideration at the federal level (the National Biometric Information Privacy Act of 2020) and in various states, including the Consumer Data Privacy Act in Pennsylvania, the Washington Privacy Act of 2021, and Assembly Bill A6787D in New York. At the municipal level, as of January 1, 2021, Portland, Oregon, became the first city to pass ordinances banning private businesses from the use of facial recognition technology. Any businesses that process or store biometric data for healthcare, security, or other applications will need to comply with these regulations in addition to more broadly applicable data privacy laws. Penalties for violating these laws can be steep. In 2021, Facebook had to pay \$650 million to settle a class action lawsuit brought under the Illinois Biometric Information Privacy Act.^[6]

Given the range and variety of data privacy regulations businesses must navigate, compliance teams need an efficient way to monitor the business's legal obligations—such as notification requirements in the event of a breach. If a business is selling to customers in five different jurisdictions that have adopted five different statutes or compliance frameworks, then the business will need a quick way to identify which set of regulations applies to which customers. However, breach notification requirements contain precise time limits, meaning that a compliance team that is stretched thin can't afford to waste time manually sifting through a trove of documents to find data privacy clauses one by one.

This is where the speed and accuracy of AI can help. Contracts are loaded with essential data about a business, from anticipated revenue to potential risks. However, that data is unstructured beyond simple clause headers. AI can provide structure to that data, making it easier to categorize, search, and analyze.

For instance, consider a clause in a vendor contract that addresses data privacy concerns but has a different name (which could be anything from "security" to "notification requirements," depending on the creativity of the people who drafted the contract). Human reviewers would need either to be directed to the relevant clause or to guess which clauses might address data privacy and review them just to be safe. That approach requires a cumbersome time commitment. AI algorithms, conversely, would not need to rely on headings to quickly review what's in each clause. Well-trained AI could instead go straight to the text of the provisions, identifying relevant clauses based on what they address instead of how they're labeled.

With quick access to detailed data on the specific notification obligations that the business has with respect to every customer, the compliance team could respond efficiently to data breaches as they arise, rather than scramble to gather information from disparate sources. This is the main benefit of AI for compliance and ethics professionals: It enables them to become proactive rather than reactive.

Contract data and ESG compliance

Another area where compliance professionals need data on the business's transactions is for environmental, social, and governance (ESG) concerns. ESG establishes sustainability standards for businesses and compliance teams to target with respect to all of their stakeholders, from consumers and shareholders to workers and local communities. It thereby offers a way for investors to evaluate companies based on their long-term prospects for sustainable and responsible profitability, rather than on short-term fluctuations and cost-cutting shortcuts.

Business and finance leaders are starting to use ESG criteria as real guidelines for investment, rather than just paying lip service to the idea. Silicon Valley's Long-Term Stock Exchange (LTSE) is leading the charge by making it easier for investors to identify and invest in companies that have committed to ESG practices. The LTSE allows dual-listing, enabling companies to secure financing from both mainstream and sustainability-focused investors through separate exchanges. In fact, the first two companies to list on the LTSE were already listed on

the New York Stock Exchange.^[7]

Qualifying to list on the LTSE, however, represents a serious commitment for businesses. Companies must first adopt enforceable policies, subject to LTSE monitoring, on issues ranging from long-term business strategy to executive and board compensation. ESG therefore can provide a set of specific, measurable objectives toward which compliance and ethics professionals should strive.

This is where contract data comes in. For example, a company seeking to list on the LTSE might need to negotiate with its suppliers to ensure that its supply chain is not creating a negative environmental impact. To ensure compliance, the buying company might require suppliers to agree to a specific clause regarding an issue such as waste disposal. ESG compliance would require that the business conduct due diligence to confirm not only that its own practices are in line with ESG standards, but also that all of the vendors that supply its inputs are leveraging environmentally responsible waste disposal practices. It's common for vendor agreements to contain ESG clauses detailing the vendor's commitments to sustainable business practices, such as obtaining and maintaining ESG certification.

When a business deals with hundreds of suppliers, however, compliance teams need an efficient way to sort through all of those vendor agreements to find which of them include the requisite ESG terms. Missing even one compliance issue with a vendor could compromise the buying company's good standing and goodwill. This is another area where contract data comes into play.

The speed and accuracy of AI can fill a gap for compliance teams that need absolute certainty regarding what's in their commercial agreements. For example, a compliance team might need to quickly ascertain what proportion of the business's vendors have represented in their contracts that they are ESG-certified. Manual review would be excessively time-consuming. AI, however, could quickly comb through thousands of contract clauses to identify the number of contracts containing ESG certification provisions and the number that do not contain them. It could also speed up the process of identifying what types of certifications different vendors have.

This document is only available to members. Please [log in](#) or [become a member](#).

[Become a Member Login](#)