DOJ Releases Updated Evaluation of Corporate Compliance Programs Guidance

International Alert
09.24.2024

On September 23, 2024, in conjunction with a related speech at the Society of Corporate Compliance and Ethics (SCCE) Compliance & Ethics Institute by Principal Deputy Assistant Attorney General (PDAAG) Nicole M. Argentieri, the U.S. Department of Justice (DOJ) released an updated version of its guidance to prosecutors on the Evaluation of Corporate Compliance Programs (updated ECCP). The DOJ last updated this guidance in March 2023. View a redline comparison of the September 2024 updates to the March 2023 version here.

The DOJ's substantive revisions for this round of updates focused primarily on using data and technology related to various compliance program elements, integrating and adapting to lessons learned from other companies, and reporting. As PDAAG Argentieri noted, the DOJ "regularly evaluate[s] our policies and enforcement tools, including the ECCP, to account for changing circumstances and new risks."

Emphasis on Data and Emerging Technology

The most substantive revisions in the DOJ's updated ECCP focus on corporate use of data and technology, covering six main issues. Some concern the risks created by emerging technologies, while others target a company's use of technology as part of its compliance program and controls. As noted by PDAAG Argentieri in her speech, the questions related to technological risks are the result of a directive from Deputy Attorney General (DAG) Lisa Monaco announced in her March 7, 2024, speech before the American Bar Association (ABA), requiring the Criminal Division to "incorporate assessment of disruptive technology risks — including risks associated with [artificial intelligence (AI)] — into its [ECCP]." The same speech also emphasized that the DOJ will seek "stiffer sentences" in cases involving the deliberate use of AI in white collar crimes.

Three sets of revisions focus on technology risks. First, in the section on Risk Assessments, the DOJ added questions designed to evaluate how a company is leveraging technology, including emerging technology such as AI, and whether a company has considered the risks of such technology. The updated ECCP states: "Where relevant, prosecutors should consider the technology—especially new and emerging technology—that the company and its employees are using to conduct company business, whether the company has conducted a risk assessment regarding the use of that technology, and whether the company has taken appropriate steps to mitigate any risk associated with the use of that technology." In short, companies should include emerging technology in their enterprise risk management (ERM) and more specific compliance risk assessment processes, adjusting their programs and controls to address the risks identified. One way to tackle this is to categorize areas where AI or related technologies are deployed, such as: the use of generative AI by employees in their day-to-day activities; in-house development of AI tools, such as for improving business processes or internal controls; in-house development of new products or software in which AI is embedded; and the purchase of such products or software from external vendors.

Second, the DOJ added a section on "Management of Emerging Risks to Ensure Compliance with Applicable Law." In this section, the DOJ sets out 10 questions focused on compliance risk management for emerging technology, including AI:

> Does the company have a process for identifying and managing emerging internal and external risks that could potentially impact the company's ability to comply with the law, including risks related to the use of new technologies?
>
> How does the company assess the potential impact of new technologies, such as artificial intelligence (AI), on its ability to comply with criminal laws?

Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management (ERM) strategies? What is the company's approach to governance regarding the use of new technologies such as AI in its commercial business and in its compliance program?

How is the company curbing any potential negative or unintended consequences resulting from the use of technologies, both in its commercial business and in its compliance program?

How is the company mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders?

To the extent that the company uses AI and similar technologies in its business or as part of its compliance program, are controls in place to monitor and ensure its trustworthiness, reliability, and use in compliance with applicable law and the company's code of conduct?

Do controls exist to ensure that the technology is used only for its intended purposes?

What baseline of human decision-making is used to assess AI?

How is accountability over use of AI monitored and enforced?

How does the company train its employees on the use of emerging technologies such as AI?

Relatedly, the DOJ added: "If the company is using new technologies such as AI in its commercial operations or compliance program, is the company monitoring and testing the technologies so that it can evaluate whether they are functioning as intended and consistent with the company's code of conduct? How quickly can the company detect and correct decisions made by AI or other new technologies that are inconsistent with the company's values?" These questions essentially frame AI as a combination of an employee, whose decisions would be subject to oversight for alignment with company values and policies, and an internal control or business process, which an effective program would typically monitor and test to confirm it is serving its intended purpose, again consistent with the company's values and policies. In both contexts, misuse of AI or its failure to follow company policies could create new risks that companies should consider and address.

Third, the DOJ added an expectation that policies and procedures are updated to reflect the use of technology. The DOJ expects companies to monitor and implement policies and procedures "that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape and the use of new technologies." This last clause serves as a reminder that more regulation over AI and other emerging technologies is on the horizon and companies will need to monitor developments to keep up.

In her speech, PDAAG Argentieri summarized the DOJ's focus on AI and related risks by noting:

> [P]rosecutors will [now] consider whether the company is vulnerable to criminal schemes enabled by new technology, ***such as false approvals and documentation generated by AI.*** If so, we will consider whether compliance controls and tools are in place to identify and mitigate those risks, such as tools to confirm the accuracy or reliability of data used by the business. We also want to know whether the company is monitoring and testing its technology to evaluate if it is functioning as intended and consistent with the company's code of conduct.

(*Emphasis added*.)

Turning to issues tied to the potential benefits of data, the DOJ's latest ECCP revisions call attention to data in third party management, asking: "Does the third-party management process function allow for the review of vendors in a timely manner? How is the company leveraging available data to evaluate vendor risk during the course of the relationship with the vendor?" These additions expand on changes made last year to ensure third party onboarding works at a speed that the business can tolerate and that third party management continues throughout the life cycle of the third party relationship.

Next, the DOJ revisions focus on ensuring that companies account for data integration in mergers and acquisitions (M&A). The updated ECCP adds the following questions for prosecutors to ask: "Does the company account for migrating or combining critical enterprise resource planning systems as part of the integration process? To what extent did compliance and risk management functions play a role in designing and executing the integration strategy?" These questions build on concepts emphasized in last year's updates to Attachment C and continue the trend to ensure the compliance function is invited to the business planning table rather than sitting on a back bench.

Finally, the Autonomy and Resources section includes new questions for prosecutors to evaluate whether compliance personnel have access to the data that they need, whether they have this access in a "timely manner," and whether the company is "appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs." Additional questions on this subject include: "How is the company managing the quality of its data sources? How is the company measuring the accuracy, precision, or recall of any data analytics models it is using?" Relatedly, under a subheading of "Proportionate Resource Allocation," the DOJ expects prosecutors to ask a series of new questions on data-related resources and usage: "How do the assets, resources, and technology available to compliance and risk management compare to those available elsewhere in the company? Is there an imbalance between the technology and resources used by the company to identify and capture market opportunities and the technology and resources used to detect and mitigate risks?" The DOJ is making clear that it expects compliance personnel to have access to the same or similar technological resources as the core business teams have. For example, if a sales team is using AI and dashboards and the compliance function is using sign-in sheets and Excel, there is work to do.

Integrating Lessons Learned

The updated ECCP emphasizes the expectation that companies will learn from the market and their industry peers, in addition to accounting for their own experiences. In the section on the design of policies and procedures, the DOJ has added that prosecutors should ask: "Is there a process for updating policies and procedures to reflect lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region? Is there a process for updating policies and procedures to address emerging risks, including those associated with the use of new technologies?" And, although a small typographical edit, the DOJ has changed its statement that "Any well-designed compliance program ***entails*** policies and procedures..." to "Any well-designed compliance program ***utilizes*** policies and procedures" (*emphasis added*), an edit that reflects the reality that policies and procedures are just two of the tools to create an effective compliance program.

Relatedly, the section previously called Training and Guidance has been renamed to Training and Communications. In that section, the DOJ has added questions related to whether training "addressed lessons learned from compliance issues faced by other companies operating in the same industry and/or geographical region." This prompt to look externally is useful, particularly the addition of the geographic region. It is important for companies to consider whether and how compliance issues faced in ***other*** industries might also affect them, to avoid the echo chamber effect that can arise when companies benchmark solely against their industry peers – only to find themselves and their peers later caught up in an industry sweep.

Reporting

In support of the DOJ's recent policy changes focused on encouraging and rewarding whistleblowers, the revised ECCP beefed up its discussion of reporting mechanisms and incentives related to reporting in the Confidential Reporting Structure and Investigation Process section. In particular, the DOJ made line edits that instruct prosecutors to ask if companies incentivize reporting of

misconduct or if they engage in practices that "chill such reporting." The DOJ would like prosecutors to look at how companies are assessing whether employees are willing to report. More significantly, the DOJ added a bullet on "Commitment to Whistleblower Protection and Anti-Retaliation" in which it asks whether companies have anti-retaliation policies, train on those policies, laws related to retaliation, and both internal and external reporting, and treat employees who reported issues differently from those who have not in disciplinary matters.

In her speech, PDAAG Argentieri summarized this area of inquiry by noting "[o]ur prosecutors will closely consider the company's commitment to whistleblower protection and anti-retaliation… as well as treatment of employees who report misconduct" and "[w]e will evaluate whether companies ensure that individuals who suspect misconduct know how to report it and feel comfortable doing so including by showing that there is no tolerance for retaliation."

Other Changes

The DOJ made various other updates in the revised ECCP. These range from adding a definition of AI in a footnote, to more substantive edits on risk assessments, which note that risk assessments should account for "emerging risks." Some other changes include:

- Tailoring training and communication to the "particular needs, interests, and values of relevant employees"
- Asking whether a company's approach to risk management is reactive or proactive
- The removal of examples for questions related to Risk-Tailored Resource Allocation
- Resource allocation and measurement of the commercial value of compliance investments
- An expansion of language dealing with post-transaction integration
- An expectation of self-assessment in responding to other types of compliance and misconduct issues

Read in coordination with Attachment C, the ECCP continues to be valuable in providing a window into the DOJ's evolving expectations and areas of focus and should serve as a prompt for corporate compliance personnel to consider whether their company's program and controls appropriately address these considerations.

For more information, please contact:

Kathryn Cameron Atkinson, katkinson@milchev.com, 202-626-5957

John E. Davis, jdavis@milchev.com, 202-626-5913

Ann Sultan, asultan@milchev.com, 202-626-1474

This alert was republished by the New York University School of Law Program on Corporate Compliance and Enforcement.
