DOJ Updates Corporate Compliance Guidance, Takes Aim at AI, Emerging Technologies, and Data Analytics

30 september 2024

Last week, the U.S. Department of Justice (DOJ) released an updated version of its Evaluation of Corporate Compliance Programs (ECCP) guidance, with key updates reinforcing the DOJ's focus on the risks associated with artificial intelligence and emerging technologies, the use of data and data analytics, and reporting processes and anti-retaliation protections. The updates, which DOJ previewed in early 2024, also highlight the need for continuous monitoring of third parties and expand upon existing guidance on learning compliance lessons from other companies.

Our team prepared a comparison to help clients and readers more easily identify the changes in the new guidance.

What is the ECCP? First published in 2017, the ECCP provides guidance on the factors federal prosecutors may consider in evaluating a corporate compliance program and a company's controls. The DOJ has since revised the ECCP several times, most recently in 2023. Although designed as a reference for prosecutors, companies have looked to the ECCP to understand the DOJ's thinking on what makes an effective compliance program and for visibility into the DOJ's current view on areas of interest.

Risks of AI and Emerging Technologies. The most significant 2024 updates to the ECCP concern identifying and managing risks around new and emerging technologies, chiefly AI. The DOJ and its leadership have been outspoken about AI risks and how the technology is changing the way crimes are committed. With the revised guidance, DOJ's core question is: *How is a company assessing and managing risks related to new technologies?* In discussing emerging technologies and compliance, the ECCP's revisions emphasize a few key themes:

- **Focus on AI.** AI, and questions about the risks associated with using AI tools, are referenced repeatedly throughout the guidance. The ECCP does not define what AI (or emerging technology) means or what such technology looks like, only referring to guidance promulgated by the Office of Management and Budget.
- **Identifying and Mitigating Technology Risks.** Companies need to identify potential risks associated with new technologies, such as AI, and to mitigate such risks. Such technologies should be specifically considered as part of enterprise risk management and annual risk assessment processes.
- **Controls and Governance.** The ECCP asks companies to evaluate controls governing the use of new technologies and mitigating potential misuse; this includes controls to ensure compliant use of AI, both when used to meet commercial needs and as part of a compliance program.
- **Understanding Technology.** The guidance also asks companies to assess how they train employees on the use of AI, "what baseline of human decision-making is used to assess the AI," and how they monitor

and control the trustworthiness and reliability of the technology.

What are the takeaways? Although the DOJ is flagging its attention to AI, it is not specifically defining AI compliance or even offering general principles of what it would look like. Most of the new language is applying existing compliance norms to this new topic. As generally true for any area of compliance, when it comes to AI, companies should think about both individual employee decisions, which should be guided by training and company policy, and business systems and processes, which should be subject to appropriate controls.

The DOJ's approach may, in some respects, resemble its approach to personal devices, ephemeral messaging, and third-party messaging platforms, which were the subject of key revision in 2023. Those updates signaled the DOJ's expectation that companies should consider the issue and develop a risk mitigation approach and that approach would be relevant in evaluating compliance programs, particularly in the event of an investigation.

When it comes to AI, companies that use or develop the technology should similarly be prepared for continued DOJ interest, should design controls to mitigate AI-related risk, and expect scrutiny in the event of an investigation—but without further specific guidance. These changes follow statements earlier this year by a senior DOJ official regarding the risks around "disruptive technology," specifically including artificial intelligence, and warnings that the DOJ may seek "stiffer sentences" where such technologies are employed and where they make crimes more serious.

The DOJ's technical interest in efforts to ensure a technology's "trustworthiness" and "reliability" also raise interesting questions. Companies should, similarly, take steps to assess these more technical points, address any issues and mitigate risks identified, and maintain a record of those efforts.

Use of Data and Data Analytics. Relatedly, the revisions also highlight the importance of using data and data analytics as part of an effective compliance program and corporate controls. The DOJ's key questions are: *Does the compliance team have access to data, and is the company appropriately leveraging its data*? This issue is highlighted in discussing several aspects of an effective compliance program, including:

- **Third-party management**: "Is the company leveraging data to evaluate vendor risk during the course of the relationship?"
- **Compliance program autonomy and resources**: "Is the company appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs?"
- **Access to data**: "To what extent does the company have access to data and information to identify potential misconduct or deficiencies in its compliance program?"
- **Compliance program evaluation, testing, and improvement**: "Prosecutors should also assess how the company has leveraged its data to gain insights into the effectiveness of its compliance program and otherwise sought to promote an organizational culture that encourages ethical conduct and a commitment to compliance…"

These additions demonstrate that the DOJ now expects companies to use data to actively monitor risks and gauge compliance program effectiveness.

Notably, in discussing the compliance program resources, the guidance includes a new heading for "Proportionate Resource Allocation." The DOJ asks how the "the assets, resources, and technology available to compliance and risk management compare to those available elsewhere in the company?" And if there is "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?" In other words, the DOJ is asking companies to perform such a direct comparison of its allocation of financial resources. While the DOJ has

long discussed the importance of an effectively resourced compliance program, this new language is more explicit about how to measure the adequacy of compliance resources.

Reporting and Anti-Retaliation. The updates include stronger language on systems to report misconduct and a new section on anti-retaliation. On the reporting mechanism (*i.e.*, compliance hotline), companies are now expected to ask if their systems "encourage" or "incentivize" reporting or if their practices "tend to chill" such behavior. A new sub-section, titled "Commitment to Whistleblower Protection and Anti-Retaliation" asks about companies' anti-retaliation policies, trainings, and even whether "employees who reported internally treated differently than others involved in misconduct who did not?"

This emphasis is consistent with the DOJ's recently-launched whistleblower rewards pilot program. Companies should take care to assess their programs in these areas, particularly training and communications (another theme in the updates) about reporting and non-retaliation.

Expanding on Existing Guidance. Two other key areas of more limited changes, where the DOJ highlights and expands upon existing guidance:

- **Heightened Expectations on Lessons Learned.** The updated ECCP adds additional references showing that the DOJ expects companies to learn from issues experienced by "*other companies* operating in the same industry and/or geographical region" (emphasis added). This concept was first added in the 2023 discussion of risk assessment, but similar language has now been added to factors companies should consider in designing policies and procedures and what companies should cover in compliance trainings. This serves as an important reminder that companies should look externally, including to recent settlements and resolutions, to better understand the risks they may face.
- **Continuous Monitoring.** With respect to third-party management, the new guidance added language asking whether the company is reviewing vendors in a timely manner and leveraging data to evaluate vendor risk "during course of the relationship." Not only does this relate to data and analytics (as discussed above), but the language is also notable for calling out the need to evaluate vendor risk even after the party was already vetted and engaged. This strengthens other recent changes about the importance of oversight of third parties.

The Bottom Line? Now is the time for companies to take a hard look at their compliance programs. These updates put companies on notice of the DOJ's current expectations and areas of interest. Compliance, legal, and other corporate leaders should assess whether and to what extent their programs already cover the issues noted above - chiefly artificial intelligence, emerging technologies, use of data and data analytics, and reporting processes and anti-retaliation protections - and take steps to address areas where program enhancement may be appropriate.