DOJ Updates Guidance on Corporate Compliance Programs to Include AI Risk Management

September 25, 2024

On September 23, 2024, the U.S. Department of Justice updated its guidance to federal prosecutors related to the "Evaluation of Corporate Compliance Programs" (the "ECCP").[1] This revision, the first since March 2023, addresses how companies manage risks associated with new and emerging technology, including artificial intelligence, and expands on preexisting guidance regarding employee reporting channels, whistleblower protection, post-acquisition compliance integration, and use of data for compliance purposes.

Noteworthy Changes to DOJ's Guidance. Federal prosecutors use the ECCP in evaluating companies' compliance programs in connection with charging decisions and penalty determinations, including whether to impose a monitor. First issued in February 2017 and revised in 2019, 2020, and 2023, the ECCP centers on three fundamental questions. In particular, the ECCP considers whether a compliance program is: (1) well designed; (2) applied earnestly and in good faith, with adequate resourcing and empowerment; and (3) working in practice.

The following are the key additions and other modifications in the latest ECCP:

- Most significantly, the updated ECCP squarely addresses the impact of new technologies, such as AI. DOJ now asks prosecutors to consider what technology a company uses to conduct business, whether the company has conducted a risk assessment regarding the use of such technology, and whether the company has taken appropriate measures to mitigate risks associated with the technology. DOJ then lists an array of follow-up considerations, including how the company assesses the potential impact of AI or other new technology on the company's ability to comply with applicable laws, what governance structure and controls the company has implemented with respect to the use of technology, what other steps the company has taken to mitigate technology-related risks and avert potential misuse

[1] U.S. Department of Justice, Criminal Division, "Evaluation of Corporate Compliance Programs" (Sept. 2024), https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.

of technology, and how the company trains its employees on the use of AI and other new technology.

- The prior ECCP already stressed the importance of an effective mechanism by which employees can anonymously or confidentially report compliance issues, as well as measures to ensure that employees who report will not be subject to retaliation. The new ECCP builds on that guidance, instructing prosecutors to consider whether and how a company incentivizes reporting (or, conversely, engages in "practices that tend to chill such reporting"), whether the company has an anti-retaliation policy, and whether the company trains employees on internal reporting channels, anti-retaliation policies and laws, external whistleblower programs, and whistleblower protection laws.

- In the transactional context, DOJ places additional emphasis on post-acquisition integration. The 2023 version of the ECCP called for assessment of a company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at an acquired entity. DOJ reinforced the importance of those considerations when it announced, later in 2023, that it will apply a presumptive six-month post-closing "safe harbor" during which an acquiring company may self-report at an acquired entity without fear of prosecution. In the new ECCP, DOJ also asks what role the compliance and risk management functions have in planning and carrying out the integration process, how the company ensures compliance oversight of the acquired business, and how the new business is integrated into the company's risk assessment procedures.

- Similarly, with regard to the use of data for compliance purposes, the new ECCP expands on DOJ's existing guidance. Specifically, prosecutors should ask not only whether a company's compliance function has sufficient access to relevant data sources but also whether the company is "appropriately leveraging data analytics tools" for compliance purposes, how the company is managing the quality of its data, and how the company is ensuring the reliability of any data analytics models it is using.

Key Takeaways for Companies. The updated ECCP's greatest impact likely will be on how companies tailor their compliance programs to address new technologies, particularly the expectation that companies will have "conducted a risk assessment regarding the use of [AI] . . . and . . . taken appropriate steps to mitigate any risk associated with the use of that technology." To meet those expectations, companies that have deployed AI for significant business or compliance operations may be asked to explain and demonstrate:

- where they have deployed AI;

- which AI use cases, if any, are high risk;
- who determines what uses are high risk and on what basis;
- the process for determining that the benefits of high-risk AI uses outweigh the risks;
- that this process includes assessing risks associated with malicious or unintended uses of the AI (e.g., through stress testing);
- for high-risk uses, the company knows the specific risks that are elevated for the particular use case (e.g., privacy, bias, transparency, quality control, vendor management, cybersecurity, loss of IP protections, regulatory compliance, contractual compliance, conflicts, etc.), and people knowledgeable about those risks have either accepted the risks or mitigated the risks (e.g., through alerts, data controls, technical guardrails, training, labeling, human review, compliance affirmations, model validation, etc.);
- high-risk uses are monitored on an ongoing basis to ensure that the risk remains acceptable or mitigated, that the AI continues to function as intended, and that significant deviations in the AI's performance are detected quickly; and
- the above process is adequately documented.

In addition, the revised ECCP puts companies on notice that, if their use of AI leads to significant compliance problems or fails to adequately identify and address those problems, as part of a charging decision, DOJ may examine the resources devoted to AI risk management and compliance. If those resources seem small compared to the resources devoted to other areas of similar risk within the company, or as a proportion of the overall expenditures on the commercial side of the AI ledger, then DOJ may find the compliance program lacking in resource allocation.

Most of DOJ's other changes to the ECCP expand on principles already articulated in the guidance and that should be integral to any well-developed compliance program. Nevertheless, by providing additional questions and specific factors for prosecutors to consider when evaluating compliance reporting channels or post-acquisition integration procedures, for example, DOJ seeks to help companies and their compliance functions more effectively design and enhance their policies, procedures, and other compliance-related tools. The ECCP remains a valuable resource not only for companies that fall under DOJ's investigative spotlight, but for any company seeking to ensure that its compliance program remains aligned with increasing regulatory expectations.

* * *

Please do not hesitate to contact us with any questions.

Helen V. Cantwell
Partner, New York
+1 212 909 6312
hcantwell@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Andrew M. Levine
Partner, New York
+1 212 909 6069
amlevine@debevoise.com

David A. O'Neil
Partner, Washington, D.C.
+1 202 383 8040
daoneil@debevoise.com

Winston M. Paes
Partner, New York
+1 212 909 6896
wmpaes@debevoise.com

Jane Shvets
Partner, New York | London
+1 212 909 6573
jshvets@debevoise.com

Douglas S. Zolkind
Partner, New York
+1 212 909 6804
dzolkind@debevoise.com

Erich O. Grosz
Counsel, New York
+1 212 909 6808
eogrosz@debevoise.com