JENNER & BLOCK

Key Insights from DOJ's September 2024 Update to "Evaluation of Corporate Compliance Programs"

Client Alerts

September 30, 2024
By: Katya Jestin, David Bitkower, Erin Schrantz, Tali R. Leinwand, Idun B. Klakegg

On September 23, 2024, the Department of Justice (DOJ) Criminal Division released its anticipated update to the "Evaluation of Corporate Compliance Programs," reflecting DOJ's recently announced measures to incentivize whistleblowers and assess compliance risks related to the use of emerging technologies such as artificial intelligence (AI). The guidance, now in its fifth iteration, replaces the March 2023 version. Like the prior versions, the September 2024 guidance seeks to make corporations aware of the criteria that DOJ uses when evaluating corporate compliance programs in the context of decisions regarding the resolution of corporate investigations. In addition to focusing on how companies encourage—or chill—reports of potential misconduct and manage the compliance risks related to emerging technologies (including AI), the guidance reinforces DOJ's expectation that compliance personnel should use data to assess whether compliance programs are effective and incorporate lessons learned from prior misconduct to improve those programs.

The updated guidance was announced by Principal Deputy Assistant Attorney General (PDAAG) Nicole M. Argentieri, who noted that the updates reflect "changing circumstances and new risks," including risks pertaining to new technology. PDAAG Argentieri also commented on DOJ's Compensation Incentives and Clawback Program, Corporate Whistleblower Awards Pilot Program (CWA), the Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP), and lessons learned from recent DOJ resolutions. As PDAAG Argentieri noted, these programs collectively reflect a broader strategy by DOJ to increase companies' incentives to invest in "robust compliance programs and report misconduct when it occurs."[1]

We highlight the following updates and changes in the September 2024 guidance:

Increased Focus on AI-Related Risks

The updated guidance provides a roadmap for federal prosecutors to assess whether companies have "appropriate guardrails"[2] around the use of emerging technologies, including AI.

The updated guidance states that companies should do more than ensure that AI tools work as intended in the company's business operations. Rather, companies should also conduct a risk assessment of their use of emerging technologies, including AI, and take measures to appropriately mitigate "any risk" associated with the use of those technologies.[3]

Specifically, the guidance directs prosecutors to consider how a company is "curbing any potential negative or unintended consequences resulting from the use of technologies, both in its commercial business and in its compliance program," and is "mitigating the potential for deliberate or reckless misuse of technologies."[4] This includes looking at the human decision-making the company uses to assess AI and how the company is enforcing and monitoring AI.[5]

As in other compliance risk areas, compliance personnel will play a critical role in helping companies establish a proper control environment to mitigate AI risks. For example, the updated guidance instructs prosecutors to assess what controls exist to ensure AI "is used only for its intended purposes," and how the company is monitoring and testing AI so it can evaluate whether the technology is functioning as intended and not running afoul of the law or the company's code of conduct.[6] Companies are also expected to train employees on the use of AI and have processes in place to "detect and correct decisions made by AI or other new technologies that are inconsistent with the company's values."[7]

Strengthening Whistleblower Protections

The updated guidance reflects DOJ's increased focus on whether companies effectively "encourage and incentivize" employees to report potential misconduct or "use practices that tend to chill such reporting."[8] Importantly, the updated guidance instructs prosecutors to evaluate how a company assesses its employees' willingness to report misconduct, consistent with DOJ's focus on how compliance personnel use data to monitor the effectiveness of compliance programs (discussed below). It is particularly noteworthy that prosecutors are now instructed to consider whether companies train their employees on internal anti-retaliation policies "as well as *external* whistleblower programs and regulatory regimes."[9] Following the recent announcement of the whistleblower awards pilot program, now is a good time for companies to revisit their internal reporting avenues and related communications to employees about how to use them.

Assessing Access to and Leveraging of Data

Continuing the trend of encouraging the use of metrics and data as a compliance tool, the updated guidance amplifies the importance of equipping compliance functions with the resources they need to effectively gather and use data to measure and improve compliance programs. The guidance asserts DOJ's interest in whether companies are "putting the same resources and technology into gathering and leveraging data for compliance purposes that they are using in their business."[10]

The updated guidance directs prosecutors to consider a number of factors, all intended to probe how a compliance function leverages data to measure the effectiveness of the company's compliance program. Those factors include whether the company is "appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs"; "managing the quality of its data sources"; "measuring the accuracy, precision, or recall of any data analytics models it is using"; and demonstrating that "it is proactively identifying either misconduct or issues with its compliance program at the earliest stage possible."[11]

Incorporating Lessons Learned

The updated guidance suggests a wider lens through which companies should view "lessons learned," extending beyond their own compliance issues to those of peer firms. For example, prosecutors are directed to consider whether a company has a process for updating policies and procedures to reflect lessons learned not only from prior *internal* issues but also from "other companies operating in the same industry and/or geographical region."[12] Similarly, companies are advised to incorporate lessons learned from compliance issues faced by those companies into their training materials.[13]

***

As the developments this month show, DOJ is continuing its push to increase expectations of corporate compliance efforts—including through the updated guidance, the Corporate Whistleblower Awards Pilot Program, the Compensation Incentives and Clawback Program, and the Corporate Enforcement and Voluntary Self-Disclosure Policy. These initiatives are meant to incentivize companies to invest in building robust compliance programs that can effectively identify and mitigate emerging risks and hold wrongdoers accountable. In light of the new guidance, corporate leaders should assess their compliance programs to ensure that they are appropriately anticipating and safeguarding against risks faced by new technologies (including AI), leveraging available data, providing robust information about internal and external whistleblower and anti-retaliation measures, and incorporating lessons learned from both within and outside the company.

Jenner & Block's Investigations, Compliance, and Defense Team has extensive experience helping companies develop and enhance corporate compliance programs that align with DOJ's expectations, reflect organizational values, and mitigate risk. We will continue to closely monitor DOJ's announcements and guidance in this area.

Footnotes

[1]Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute | OPA | Department of Justice

[2]Update on Deputy Attorney General Lisa Monaco's Justice AI Convenings | OPA | Department of Justice

[3]Evaluation of Corporate Compliance Programs, Department of Justice (Sept. 2024), at 3-4.

[4]*Id.* at 4.

[5]*Id.*

[6] *Id.*

[7] *Id.* at 18.

[8] *Id.* at 7.

[9] *Id.* at 7 (emphasis added).

[10] Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute | United States Department of Justice.

[11] Evaluation of Corporate Compliance Programs, Department of Justice (Sept. 2024), at 13, 19.

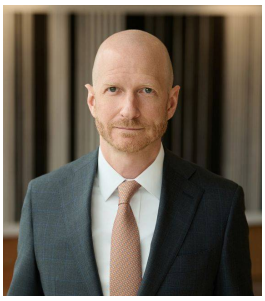
[12] *Id.* at 4.

[13] *Id.* at 6.

Related Lawyers



Katya Jestin
Partner
kjestin@jenner.com
+1 212 891 1685



David Bitkower
Partner
dbitkower@jenner.com
+1 202 639 6048



Erin Schrantz
Partner
eschrantz@jenner.com
+1 312 840 8674



Tali R. Leinwand
Partner
tleinwand@jenner.com
+1 212 891 1697



Idun B. Klakegg
Associate
iklakegg@jenner.com
+1 212 407 1744

Related Capabilities

Investigations, Compliance, and Defense

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →