BCLP. Client Intelligent

Insights

UPDATED DOJ COMPLIANCE GUIDANCE MUST BE REVIEWED AND IMPLEMENTED IN LIGHT OF PRIVACY REGULATIONS

Jul 09, 2020

In June, the U.S. Department of Justice updated its Evaluation of Corporate Compliance Programs Guidance ("Guidance"). While the Guidance is intended to assist prosecutors by providing factors to consider in evaluating the effectiveness of a company's compliance program in the context of a criminal investigation, it also is a useful tool for companies implementing and evaluating compliance policies, procedures, and practices. Nonetheless, companies need to consider the recommendations contained in the Guidance in light of other legal requirements, such has privacy laws, and ensure that they can demonstrate a rationale for the compliance decisions that they make.

The updates to the Guidance are not major changes to the structure of the Guidance. Instead, they largely focus on ensuring a company's compliance function is appropriately resourced, including through accessing data to monitor, test, evaluate, and update the program to reflect changing conditions and risks. Yet, as with any recommended data collection effort by a company, an effort that the updates to the Guidance definitely support, companies must ensure that their collection of data complies with complicated laws protecting the privacy of their employees.

For example, one sentence DOJ added to the Accessibility section of the Guidance may appear harmless, but actually could create problems in countries that have strict data privacy laws. In addition to recommending that a company make its policies and procedures available to all employees and relevant third parties, the update asks "Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?" While such tracking may be permissible under U.S. federal law, depending on the jurisdictions in which an entity is operating and the various privacy laws that may attach to a company or its employees or affiliates, such tracking may require, at minimum, substantial warnings. For example, if a company elects to collect data that Employee X has clicked on Policy Y 20 times in the past month, retaining that data may violate specific laws regarding data privacy. The concern increases if the data compiled can be tied to a specific person, which would likely be necessary if one wanted to be able to assess "relevant" employees. We doubt that DOJ considered the potential implications of this recommendation under other privacy regimes, but it underscores

the importance of evaluating guidance, including that that contained in these updates, as one factor in the broader context of assessing your company' s compliance risks and protocols.

The updates' focus on ensuring that a compliance program is appropriately resourced starts from the very beginning of the Guidance and is a theme throughout. In determining whether a program is effectively implemented, the updates clarify: "In other words, is the program being adequately resourced and empowered to function effectively?" That change focuses a DOJ review on the resources and authority of the compliance department within the company. As such, these changes essentially recommend giving more authority and resources to a company's compliance personnel. For example, the DOJ adds a question – "How does the company invest in further training and development of the compliance and other control personnel?" The updates suggest that DOJ wants to see more resources going to the compliance personnel. To the extent that the compliance department is subordinate to others, DOJ wants the company to be able to demonstrate "the reasons for the structural choices the company has made." All of this reflects the reality that the most robust compliance program on paper does not add value to an organization if that program is not implemented and if those tasked with that implementation are not given the necessary tools and autonomy to do so.

To that end, the Guidance looks to both the ongoing development of compliance personnel and the ability of those personnel to evaluate company operations and use that data to improve the compliance program. In other words, DOJ encourages companies to create an active feedback loop within the compliance program itself so that it is constantly improving. This feedback should include regular risk assessments as well as lessons learned from the company and from other entities operating in the same industry and/or geographical area.

The risk assessment and monitoring processes must be robust by making them more data-driven and fact-intensive. The modifications set out that data must be collected from at least three different areas: (1) from the whistleblower hotline; (2) from its training sessions; and (3) from investigations and disciplinary actions. Not only should the company collect data, but the compliance and control persons must have access to the data – the DOJ adds an entire new paragraph on compliance persons' access to the data.

Three other updates are worth mentioning. First, DOJ now explicitly recognizes that training sessions often reveal issues – so they encourage in-person training sessions in which employees can ask questions and compliance personnel can identify potential concerns or areas of risk based on their interactions with business people. Second, on third party due diligence, the updates make it clear that DOJ wants to see continuing due diligence – not just due diligence done on the on-boarding process. Finally, DOJ makes several changes to the mergers & acquisition section of the Guidance to clarify that pre-acquisition due diligence is not sufficient – the compliance program should also include measures to ensure that the acquired company is swiftly integrated within the compliance program and to ensure that is done by conducting post acquisition due diligence.

In the end, the DOJ wants to see to see a living, evolving compliance program. They do not want one that was a “snapshot” frozen in time. Only then can the program address the risks that the company actually faces. The Investigations, Financial Regulation and White Collar Team at BCLP can assist your company in ensuring your company’s compliance program considers the DOJ’s Guidance in this area.

RELATED CAPABILITIES

- White Collar
- Investigations
- Data Privacy & Security

MEET THE TEAM

Mark A. Srere

Washington

mark.srere@bclplaw.com
+1 202 508 6050

Jennifer Kies Mammen

Washington

jennifer.mammen@bclplaw.com
+1 202 508 6044
