Blogs
December 15, 2017

As cybersecurity concerns move more companies to batten down employee use of external email accounts and other websites through blocking software and other measures, the DOJ's recently issued FCPA Corporate Enforcement Policy—now incorporated in the U.S. Attorneys' Manual—unequivocally states that companies seeking full cooperation credit from DOJ in FCPA cases must ensure that employees are prohibited "from using software that generates but does not appropriately retain business records or communications," among other business-record retention measures.

Even setting aside the difficulties in policing "old" technology such as personal email accounts and text messaging on employee-owned devices, the constant evolution and emergence of new electronic messaging platforms will undoubtedly create significant challenges for companies seeking to satisfy DOJ's expectations. Former FCPA Unit prosecutor Pat Pericak—now a Senior Managing Director at FTI Consulting—acknowledged the difficulties that companies are likely to face in policing employee electronic communications, particularly on devices that are not owned or controlled by the corporation. That said, Pericak believes that there are a number of actions within a company's control that would demonstrate a good-faith effort to meet the standard set forth by the DOJ's updated policy. Specifically, companies can:

1. Ensure internal policies require that employees use their company-owned devices and not their personal devices for communications and storage of company records (with reasonable exceptions to accommodate emergency situations);
2. Ensure that company devices are programmed and monitored to block the installation of software that is not in conformance with DOJ expectations on data retention;
3. Within the confines of the relevant jurisdiction's data privacy and employment laws, periodically spot-check or request self-certifications to make sure that employees are not using personal devices;
4. Encourage employees to report violations of company policies, including violations of any policy prohibiting the use of personal devices for company communications and storage of company records; and
5. Meaningfully discipline employees who violate the policy.

Given the myriad obstacles companies face in policing, retaining and collecting data from foreign locations, the DOJ's latest move only raises the bar higher. Companies conducting business outside the U.S. should be aware that the DOJ is not dialing back its hefty expectations, notwithstanding the very real challenges ahead.

Explore more in

White Collar & Investigations
Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie’s White Collar and Investigations group highlights key considerations and offers practical insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.

View the blog