BURR FORMAN LLP

Department of Justice Expectations on Corporate Compliance Programs Concerning Use of Personal Device and Messaging Applications for Business Purposes

Article
05.16.2023

Are your employees conducting business by exchanging text messages on personal devices or communicating using messaging applications? If so, it may be time to evaluate your compliance and document retention policies.

Today's workforce increasingly rely on employees to use personal devices and messaging applications for business communications, and employees are able to access software and data on personal devices. But how will that impact your business if you find yourself facing an investigation by a state or federal government agency?

In September 2022, the Department of Justice (DOJ) announced several significant updates to its corporate criminal enforcement policy. At that time, DOJ expressed concern over the use of certain messaging applications, including encrypted and ephemeral messaging applications such as WhatsApp, Signal and Telegram, by company employees for business purposes. Of particular concern is the unofficial use of these platforms, which may not be captured by the corporation's document retention policies, but use of said platforms may be necessary data and information for audits, reviews or investigations.

More recently in March 2023, at the American Bar Association's 38th Annual National Institute on White Collar Crime, the DOJ issued revisions to its Evaluation of Corporate Compliance Programs (ECCP). The newly revised ECCP guidance contains

RELATED PROFESSIONALS

Robin Beardsley Mark

RELATED CAPABILITIES

Corporate Law

Cybersecurity & Data Privacy

Department of Justice Expectations on Corporate Compliance Programs Concerning Use of Personal Device and Messaging Applications for Business Purposes

important information on how the DOJ will evaluate corporate practices surrounding the use of personal devices, communication platforms and messaging applications and a corporation's ability to access, preserve and produce data.

In evaluating a corporation's compliance policy, the DOJ will consider:

- How policies relating to personal devices and messaging applications are tailored to a company's specific risk profile.
- How policies ensure that business-related data can be preserved and accessed.
- How policies are communicated to employees.
- How companies monitor and enforce compliance by employees.

In light of these recent updates to the DOJ corporate enforcement policy, companies need to develop and implement comprehensive policies and procedures addressing remote access, the use of personal devices, and messaging applications to ensure data and business communications can be accessed and preserved appropriately. Without a sound policy on remote access and personal devices, companies may be left exposed to the growing number of off-the-clock lawsuits, data ownership issues, and cybersecurity risks associated with remote access and personal device use. The bottom line is companies need to know how their employees are communicating and be able to access and preserve business related data and communications from whatever device or platform their employees may be utilizing.

So, what actions can you take to protect yourself and your company? The following is a list of best practices that you can use to evaluate your corporation's communications policy.

Audit: Review the current authorized and unauthorized business communications and collaboration platforms and devices that employees are using in the ordinary course of business. Determine the record retention capabilities of various platforms and deficiencies.

Research Solutions: Identify easy to use collaboration and communications platforms, and discourage use of unauthorized platforms. Authorized platforms should have retention capabilities.

Implement Policies: Implement a clear policy on use or prohibition of personal devices and messaging platforms. The policy should include review of personal devices by the company upon request.

Know Your Corporate Record Keeping Obligations: Understand and comply with all laws mandating retention of records.

Train Employees: Train employees on the risks associated with use of personal devices, preservation of records and unauthorized platforms.

Department of Justice Expectations on Corporate Compliance Programs Concerning Use of Personal Device and Messaging Applications for Business Purposes

Monitor and Enforce Compliance: Enforce violations with appropriate discipline, regardless of employee's status within the company.