Data Privacy Compliance Basics: ICYMI Webinar Recap

By:Kevin S. Olson
February 15, 2023

As part of the Morse Women Attorneys Webinar Series, Faith Kasparian, Ann O'Rourke, and Rebecca Alperin hosted an interactive 'true or false' session to bring attendees up-to-speed on data privacy compliance basics. Each session in the series focuses on an area of law essential to the business lifecycle, start to exit and everything in between. (Don't miss the next one, register here!)

Faith opened the session with a reminder that businesses need to remember that privacy is not *only* about doing right by your customers. Privacy compliance matters for a number of other reasons such as: building trust in the market; sophisticated business customers will often demand compliance; there can be harsh penalties from regulators; and it is an area of focus in the investment and merger/acquisition context.

Ann provided a key breakdown of the international divide in how privacy rights are codified. The United States often takes a consumer protection approach to privacy and has a patchwork of national and state laws that often creates compliance headaches, on the other hand, the European Union views privacy as a fundamental right and has enacted omnibus privacy legislation in the form of the General Data Protection Regulation (GDPR).

However, things in the U.S. are changing with new state laws in California, Colorado, Connecticut, Utah, and Virginia (that borrow from the EU approach) and grant certain data subject rights and place different obligations on business depending on their role. One tricky thing to remember is that a business can (and often is) be both a "controller" and a "processor" with respect to data it handles.

While there are a multitude of complex laws and regulations to deal with, Faith offered a helpful tip that most privacy laws are based on common principles known as the Fair Information Practices (FIPs). Adhering to the FIPs at an organizational level can make compliance with specific laws a much simpler process!

And for any businesses that offer employee benefit plans, Rebecca advised attendees that benefit plan fiduciaries have a legal duty to mitigate cybersecurity risk. Although cybersecurity and employee benefit plans might not seem like overlapping areas, employee benefit plans often have plenty of sensitive personal information like bank account information, investment information, health and health insurance data, and Social Security numbers. This means that all plan fiduciaries (and vendors) need to be taking action to address cybersecurity risks.

If you have questions about data privacy and security compliance, contact Faith Kasparian, Ann O'Rourke, Rebecca Alperin, or Kevin Olson.

Also, be on the lookout for upcoming events in this series, including another webinar hosted by Rebecca on March 9th, providing a general overview of the Internal Revenue Code and ERISA

requirements applicable to qualified plans, and a future event regarding Intellectual Property!

Join the invite list.