May 23, 2018

GDPR: Data Privacy Taken to the Next Level

Effective May 25, 2018, the European Union (EU) General Data Protection Regulation (the GDPR) will have a far reaching effect on data privacy. The GDPR will not only affect companies located in the EU, but it will apply to any company that offers goods or services to the EU or monitors the behavior of people in the EU (e.g. social media sites). Additionally, the UK currently has a data protection bill in the works that is similar to the GDPR.

The goal of the GDPR is to improve the security and protection of personal data by implementing:

- Stronger requirements for an individual to provide consent to such individual's disclosure of personal data to companies, including the ability to withdraw consent.

- The ability for individuals to have access to their data and the right to request for the deletion of their data for a number of reasons, including due to the data being obtained through unlawful means.

- New laws regarding profiling, handling of sensitive data and data retention in order to restrict what companies may do with the data they collect and how they store and manage such data.

- Increased liability of data processors (companies that process personal data on behalf of other companies), including obligations for them to maintain certain documentation, security standards and data protection assessments.

- A requirement for companies to notify data protection authorities of data breaches within 72 hours and individuals without undue delay.

- Increased obligations on data controllers to show compliance with GDPR.

Consequently, companies falling within the law's jurisdiction will need to improve their standards for data processing and retention. Failure to comply with GDPR can lead to significant sanctions, including fines of up to 4% of annual global turnover or €20 million, whichever is higher. Data protection authorities will have increased powers to conduct audits

regarding data protection, and the GDPR will make it easier for individuals to bring private lawsuits against companies related to their data privacy.

In order to comply with GDPR, companies will need to implement new privacy policies or amend existing policies, and may even need to change their business operations and data security platforms. Companies and organizations, including investment advisors and private funds, will need to implement a compliance framework that shows they are taking active measures to ensure effective data protection, including documentation, regular audit processes and a method for detecting and reporting a data breach. They should also provide a privacy disclosure to their clients that describes the way they process data and the statutory rights available to their clients. Companies are encouraged to consult with counsel and regulatory consultants for further information.

For more information about complying with the GDPR, contact any member of the Investment Management Practice Group.

Contacts

James W. Van Horn, Jr.
Partner
804.771.9541
jvanhorn@hf-law.com

Alina A. Savage
Associate
804.771.5694
asavage@hf-law.com