New data security laws in New York State impact businesses with residents' personal information

With the enactment of the SHIELD Act in 2019 came rapid changes to then-existing data breach notification requirements in New York State, which became effective in the fall of 2019. Now, a second compliance date of March 21, 2020 has recently passed, bringing with it another wave of sweeping changes with new substantive requirements dedicated to hardening information security and data protection specifically. Entities maintaining personally identifiable information of New York State residents must comply with these requirements.

About half of all states already require businesses to implement "reasonable" security measures to protect the information of their respective residents. But the lack of specificity in these other statutes leaves plenty of wiggle room when it comes to compliance. With the passage of the SHIELD Act, New York is imposing more specific requirements for data security on all businesses, regardless of industry.

The SHIELD Act categorizes its new requirements into administrative, technical, and physical safeguards. Although businesses must be mindful of all of them, two requirements are especially noteworthy.

First, the SHIELD Act requires businesses to securely dispose of information containing personally identifiable information when the information is no longer needed for business purposes. This data disposal requirement can be cumbersome, not just because it is unique to New York, but because access to data storage in the cloud means that storage parameters have become virtually limitless and, coupled with the low cost of storage, keeping information indefinitely has become the norm.

Second, the SHIELD Act also requires businesses to select third-party service providers who themselves employ appropriate cybersecurity protections and require those protections by contract. This requirement necessitates a review and analysis of all new and existing service provider agreements.

If businesses have not already taken a critical eye to their current data protection policies and practices to ensure compliance with the SHIELD Act, now is the time to do so.

For more information on this topic, please contact Daniel J. Altieri, Senior Associate at Harter Secrest & Emery LLP, at DAltieri@hselaw.com or Anna S.M. McCarthy, Associate at Harter Secrest and Emery LLP, at AMcCarthy@hselaw.com or 716.853.1616.