KRESTON
EZRA YEHUDA-ROZENBLUM
CONSULTING, CONTROL & RISK MANAGEMENT

Are you Cyber ready for the NYS Shield act?

The NY SHIELD ACT

In July 2019, the New York State Senate passed the "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act to increase cyber security protections. The law applies to any person or business operating in New York in connection with owning or licensing electronic personal private data.

The SHIELD Act requires companies to have comprehensive programming in place to prevent breaches, have training programs in place, and regularly monitor their controls for effectiveness. The SHIELD Act also significantly expands the definitions of a breach and private information, the companies the law applies to, and the reporting period.

Compliance with the SHIELD Act is required by March 21, 2020.

What does this mean for your firm?

Businesses that own or license personal information of New York State residents are now required to implement "reasonable safeguards" preventing breach of that information.

What are considered required "reasonable safeguards" according to the New York Senate?

- Ensure your breach notification policy includes notice to New York residents and make any necessary updates
- Designate one or more employees to coordinate your security program
- Detect, prevent and respond to attacks or system failures
- Regularly test and monitor the effectiveness of key controls, systems and procedures
- Identify reasonably foreseeable internal and external risks, including risks in network and software design and risks in information processing, transmission and storage
- Assess the sufficiency of safeguards in place to control the identified risks
- Train and manage employees in the security program practices and procedures
- Select service providers capable of maintaining appropriate safeguards
- Adjust your security program in light of business changes or new circumstances
- Protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information
- Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Penalties are subject to a tier structure, however, if a business chooses to completely ignore the SHIELD Act's requirements, fines could be up to $250,000.

Kreston cybersecurity and compliance solutions are designed to help clients meet regulatory requirements. We can help you assess if your current policies and security program comply with the SHIELD Act and assist you in implementing additional safeguards to validate your organizations effectiveness to comply with various regulations, as well as other business requirements.

Contact Kreston to schedule a consultation to ensure you are prepared for the SHIELD ACT.

Phone: 03-6130632

Email: office@kreston.co.il