New York SHIELD Act Raises Bar for Data Privacy and Security

As US legislators struggle to agree on a comprehensive federal data privacy and security law, New York has joined a growing chorus of states implementing their own laws. The New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) was signed into law on July 25, 2019, and became effective on March 21, 2020. The new law requires companies to implement a "cybersecurity program" to reduce risks of a data breach.

The Act amends New York's general business law and state technology law, raising the bar for protection of personal information and notification of a security breach. Here are some of the key changes:

- Expands definition of "private information" to include information such as biometric data and username/email address in combination with a password or security questions and answers.
- Broadens definition of "data breach" to include unauthorized "access to or acquisition of" data. Prior to this amendment, the definition was limited to "acquisition of" data, which set a higher burden of proof for a data breach. With this amendment, an incident in which cybercriminals have *access* to data may qualify as a data breach, even if there is no evidence that the attackers *acquired*—or exfiltrated—the data.
- Lengthens timeframe in which New York attorney general may bring action in response to a SHIELDS Act violation from two years to three years from the date of breach notification, or the date the attorney general became aware of the violation, whichever occurs first.
- Increases penalties for failure to notify affected persons of a data breach to the greater of $5,000 or $20 per incident, up to a maximum amount of $250,000.

Who's Impacted?

Any person or business owning or licensing computerized data that includes private information about New York residents will be subject to the new law. This includes biometric data, unsecured health data, financial account numbers, and email addresses that are linked to passwords or security questions/answers.

The Act applies to all New York businesses, as well as businesses outside of New York, that use private information pertaining to New York residents.

Data Breach Notification Requirements

Under the SHIELD Act, businesses must notify New York residents when their private information may have been compromised in a data breach. The notification must occur "in the most expedient time possible and without reasonable delay." Notably, the new law requires notification when the private information has merely been "accessed," even if there is no evidence that the information was "acquired" by unauthorized parties. This may significantly increase the number of breaches that will require notification.

If the data breach incident involves the private information of over 500 New York residents, the breached business must provide documentation to the New York attorney general within ten business days after the breach determination.

Security and Data Privacy Requirements

The SHIELD Act requires businesses to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information about New York residents. Three types of safeguards are required: Administrative, Technical, and Physical.

Administrative Safeguards

- Designate one or more employees to coordinate the cybersecurity program.
- Assess internal and external security risks and the sufficiency of existing safeguards to control the identified risks.
- Train and manage employees in security program practices and procedures.
- Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract.
- Adjust the security program in light of business changes or new circumstances.

Technical Safeguards

- Assess risks in network and software design.
- Assess risks in information processing, transmission, and storage.
- Detect, prevent, and respond to attacks or system failures.
- Regularly test and monitor the effectiveness of key controls, systems, and procedures.

Physical Safeguards

- Assess risks of information storage and disposal.
- Detect, prevent, and respond to intrusions.

- 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.

Relief for Small Businesses

Small businesses with fewer than 50 employees and less than $3 million in gross annual revenue in the past three years or less than $5 million in total assets at year-end have some relief under the SHIELD Act. They are simply required to implement "reasonable" administrative, technical, and physical safeguards that are appropriate based on the businesses size and complexity and the sensitivity of the data they use. Businesses that exceed theses thresholds must meet all requirements described in the new Act.

Tevora Can Help

If you'd like help understanding the SHIELD Act requirements in more detail, or making changes to your environment to ensure you're in compliance, our expert team of security specialists is here to help. Just give us a call at (833) 292-1609 or email us at sales@tevora.com.