INNOVATIVE TECHNOLOGIES

What Businesses Need To Know About The NYS SHIELD ACT

Provided as an educational service by:
Paul Tracey – CEO/Owner
Innovative Technologies
WWW.UpstateTechSupport.com
(518) 900-7004

Introduction

The New York State SHIELD Act, which stands for "Stop Hacks and Improve Electronic Data Security Act," was signed into law on July 25, 2019, by Governor Andrew Cuomo.

The new law amended New York's 2005 Information Security Breach and Notification Act and significantly strengthens New York's data-security laws.

It is designed to protect the personal information of New York residents by imposing specific data security and breach notification requirements on businesses.

This law applies to any business that collects or stores the personal information of New York residents, regardless of whether the business operates in New York or not.

Under the SHIELD Act, businesses must implement reasonable data security measures to protect personal information from unauthorized access, use, disclosure, or destruction.

Additionally, if a data breach occurs, businesses must provide timely notification to affected individuals, the New York Attorney General, and any other relevant government agencies.

How Has The SHIELD Act Changed The Previous Law?

The first thing The SHIELD Act does is substantially expanded the original law's meaning of "Private Information". The original law only considered social security numbers, driver's license numbers, credit or debit card numbers, or financial account numbers to be protected information.

Because of our increasingly complicated technology landscape, The SHIELD Act now includes biometric information, email addresses, and corresponding passwords or security questions and answers along with financial account numbers without a required security code if an unauthorized person could access the account.

Secondly, the definition of a data breach has been expanded to include bad actors with authorized access rather than solely focusing on unauthorized access.

A breach in security does not include "good faith access to, acquisition of private information by an employee or agent of the business" as long as the data is not used or subject to unauthorized disclosure.

Do you have more questions? Claim your FREE Discovery Call NOW!
www.UpstateTechSupport.com/DiscoveryCall/
Or call our office at (518) 900-7004**.**

Who Does The SHIELD Act Affect?

Broadly, The SHIELD Act requires "any person or business" that owns or licenses computerized data, which includes private information of a New York resident, "shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information, including, but limited to, the disposal of the data."

However, entities with a data security program compliant under the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and/or the New York State Department of Financial Services Cybersecurity Regulation are exempt as these laws have higher thresholds to meet for compliance than The SHIELD Act.

The other exemption is for small businesses that must scale their data security requirements according to their size and complexity, the nature and scope of business activities, and the nature and sensitivity of the information collection.

What Requirements Are Put In Place By The SHIELD Act?

The SHIELD Act requires ANY person or business that maintains private information to adopt administrative, technical, and physical safeguards.

The act lists some safeguards but is not meant to be an exhaustive list.

Reasonable Administrative Safeguards:

1.)Designating one or more employees to coordinate the security program

2.) Identifying reasonably foreseeable internal and external risks

3.) Assessing the sufficiency of safeguards in place to control the identified risks

4.) Training and managing employees in the security program's practices and procedures

5.) Selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract

6.) Adjusting the security program in light of any business changes or new circumstances

Reasonable Technical Safeguards:

1.) Assessing risks in network and software design

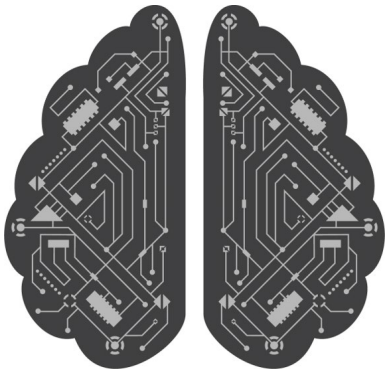
2.) Assessing risks in information processing, transmission and storage

3.) Detecting, preventing, and responding to attacks or system failures

4.) Regularly testing and monitoring the effectiveness of key controls, systems, and procedures

Do you have more questions? Claim your FREE Discovery Call NOW!
www.UpstateTechSupport.com/DiscoveryCall/
Or call our office at (518) 900-7004**.**

Reasonable Physical Safeguards:



1.) Assessing risks of information storage and disposal

2.) Detecting, preventing, and responding to intrusions

3.) Protecting against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of information

4.) Disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing

The Obligations Of Businesses When A Breach Occurs:

The law requires that the person or business notify the affected consumers following discovery of the breach in the security of its computer data system affecting private information.

The disclosure must be made in the most expedient time possible consistent with legitimate needs of law enforcement agencies.

The law requires notice to the Attorney General's office, New York Department of State and the New York State Police of the timing, content and distribution of the notices and approximate number of affected persons.

Submitting a breach form through the NYAG data breach reporting portal is sufficient as that form is automatically sent to all three entities.

Breach Notification Requirements:

The person or business must also notify consumer reporting agencies if more than 5,000 New York residents are to be notified. The contact information for the three nationwide consumer reporting agencies is as follows:

EXPERIAN
Consumer Fraud Assistance
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

EQUIFAX
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
www.equifax.com

TRANSUNION
P.O. Box 2000
Chester, PA 19016
Phone: 800-909-8872
www.transunion.com

The law also provides for substitute notice to consumers if the business demonstrates to the Attorney General that the cost of providing regular notice would exceed $250,000 or that the affected class of persons exceeds 500,000 or the entity or business does not have sufficient contact information.

Where substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity's web site, and notification to statewide media.

What Are The Penalties For Violations Of The SHIELD Act?

Under The SHIELD Act, the Attorney General may seek injunctive relief, restitution and penalties against any business entity for violating the law.

For failure to provide timely notification, the court may impose a civil penalty of up to $20 per instance of failed notification not to exceed $250,000.

For failure to maintain reasonable safeguards, the court may impose a civil penalty of up to $5,000 per violation.

Would You Like To Set Up A Free Call With Us?

If you have any questions about what you read today, we'd like to answer them. On this call we can discuss your unique situation, any concerns you have and of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our proprietary Cybersecurity Risk Assessment.

This Assessment can be conducted 100% remotely with or without your current I.T. company or department knowing (we can give you the full details on our initial consultation call).

At the end of the Assessment, you'll know:

- Where you are overpaying (or getting underserved) for the services and support you are currently getting from your current I.T. company or team.
- Whether or not your systems and data are *truly* secured from hackers and ransomware, and where you are partially or totally exposed.
- If your data is *actually* being backed up in a manner that would allow you to recover it quickly in the event of an emergency or ransomware attack.
- Where you are unknowingly violating specific New York state or federal laws.
- How you could lower the overall costs of I.T. while improving communication, security and performance, as well as the productivity of your employees.

Fresh eyes see things that others cannot – so at a minimum, our free Assessment is a completely risk-free way to get a credible third-party validation of the security, stability and efficiency of your I.T. systems.

Do you have more questions? Claim your FREE Discovery Call NOW!

www.UpstateTechSupport.com/DiscoveryCall/

Or call our office at (518) 900-7004**.**