COMPLIANCE BRIEF
New York SHIELD Act

Data privacy regulation affecting any entity that processes private information of residents of New York

What is the New York SHIELD Act and Why Is It Important?

The Stop Hacks and Improve Electronic Data Security Handling ("SHIELD") Act was introduced to address the ever-increasing threat of data breaches occurring in the State of New York. It applies to ***any entity*** that processes the private information of residents of New York ***regardless of where that entity is located***. If your business is located outside of New York State (or even outside of the United States), compliance with the SHIELD Act will be *mandatory* if *private information* of a resident of New York State is being processed.

Private information includes social security numbers, driver's license number, credit or debit card information, biometric information and username or e-mail addresses with a password.

Organizations that are subject to the following data protection regimes are deemed to already comply with the SHIELD Act; Gramm Leach Bliley Act (GLBA); HIPPA and New York State Department of Financial Services Cybersecurity Regulation.

WHAT BUSINESSES NEED TO KNOW

The SHIELD Act updates existing data protection legislation to ensure more stringent requirements and tighter controls are adopted by businesses regarding data security.

1. Data Breach Notification requirements have expanded in scope from previous data protection legislation.

   Once it has become apparent that a data breach has occurred (meaning that the private data of a resident of New York State was accessed or acquired without valid authorization) an organization shall notify the individual concerned and provide the following information:

   (A) Its contact information; (B) the telephone numbers and websites of government agencies that provide information regarding data breach responses; and (C) a description of the categories of information that was breached, specifying what was personal or private information.

2. Data Security Requirements have been introduced. Any individual or entity that processes the personal data of residents of New York must '*develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information'.*

   The Data Breach Notification requirements came into effect on October 23rd, 2019 and the Data Security Requirements come into effect on March 22, 2020.

CIVIL PENALTES

For failure to comply with Data Breach Notification requirements, a court may impose penalties on an organization of up to $20 for each incident of a failed notification, to a maximum of $250,000.

WHAT SHOULD YOU DO NEXT?

While full a compliance assessment and action plan should be carried out, some recommended priority actions are:

- Define and manage a process to ensure breach notification requirements are met. Have an established procedure to be undertaken in the event that a data breach occurs. Who in your organization will own this process?
- Undertake a data-mapping exercise to understand what categories of 'private information' your organization holds.
- Define and document a comprehensive Information Security Policy and Procedure to ensure that your organization is adopting 'reasonable safeguards' to protect the *security, confidentiality and integrity of the private information'.*

A copy of the NY SHIELD act can be found here:

https://www.nysenate.gov/legislation/bills/2019/S5575

CERTES NETWORKS

Contact Certes Networks
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com