GUNDERSON DETTMER

New York to Require New Data Security Measures Under the SHIELD Act on March 21, 2020

Insights
February 27, 2020

The New York Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") requires companies to adopt data security measures and notify New York residents in the event of a data breach. This client alert provides guidance on the scope and compliance requirements of the SHIELD Act's data security sections, which will take effect on March 21, 2020.

Companies Subject to the SHIELD Act

The SHIELD Act applies to companies that have the "private information" of New York residents. Any company with such private information must comply with the law, even if not based in New York. "Private information" means the following unencrypted combination of information:

- Personal information that can identify a New York resident, **AND** one or more of the following:

  - Social security number.

  - Driver's license or non-driver identification card number.

  - Account number or credit or debit card number, where that information could be used either alone or in combination with other information (like a password, security code, access code, etc.) to access to an individual's financial account.

- Biometric information, such as fingerprints, that could be used to authenticate or ascertain an individual's identity.

- A username or email address in combination with a password or security question response that would permit access to an individual's online account.

Data Security Requirements

Covered companies must have reasonable measures to protect the security, confidentiality, and integrity of private information. Companies can meet this obligation one of in two ways:

- Comply with another recognized data security regime, including those set out in:

  - The Gramm-Leach-Bliley Act (for financial data)

  - The Health Insurance Portability and Accountability Act

  - The New York Department of Financial Services Cybersecurity Regulations

- Implement reasonable administrative, technical and physical safeguards. The law provides the following examples of each,

  - Administrative Safeguards:

    - Designating one or more employees to coordinate the security program.
    - Identifying reasonably foreseeable internal and external risks.
    - Assessing the sufficiency of safeguards in place to control the identified risks.
    - Training and managing employees in the security program practices and procedures.
    - Selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract.
    - Adjusting the security program in light of business changes or new circumstances.

  - Technical Safeguards:

    - Assessing risks in network and software design.
    - Assessing risks in information processing, transmission and storage.

- Detecting, preventing and responding to attacks or system failures.
- Regularly testing and monitoring the effectiveness of key controls, systems and procedures.

- Physical Safeguards:

- Assessing risks of information storage and disposal.
- Detecting, preventing and responding to intrusions.
- Protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information.
- Disposing 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.

Companies should maintain a written data security protection program and document their compliance efforts.

Small companies – those with fewer than 50 employees, less than $3,000,000 in gross annual revenue in each of the last 3 years, or less than $5,000,000 in year-end total assets – should adjust their data security program so that the administrative, technical, and physical safeguards they use are appropriate for the size of the company, the company's business, and the sensitivity of the personal information the company collects.

Breach Notification Requirements

Responding to a data breach is time sensitive and likely to include specific regulatory requirements. If you discover that you may have had a data breach, contact your GD attorney immediately. In addition to potential liability under the SHIELD Act, you may be exposed to liability pursuant to other data privacy and security laws, and contractual liability with your customers.

Penalties for Non-Compliance

While the SHIELD Act does not contain a private right of action, the New York Attorney General can impose injunctive relief and fines.

- Data security: Failure to implement reasonable data security measures may result in civil penalties of up to $5,000 for each violation.

- Breach notification: Failure to comply with the SHIELD Act's breach notification requirements may result in damages for actual costs or losses to the person, including consequential financial losses. For knowing or reckless failure to provide notification, the penalty may be the greater of $5,000 or $20 per instance of failed notification, with a cap of $250,000.

LEGAL DISCLAIMER

Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP provides these materials for information purposes only and not as legal advice. The Firm does not intend to create an attorney-client relationship with you, and you should not assume such a relationship or act on any material from these pages without seeking professional counsel.

ATTORNEY ADVERTISING

The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice. Our website may contain attorney advertising as defined by laws of various states.

Related People

Katherine S. Gardner
PARTNER
P +1 212 430 3188

Anna C. Westfelt
PARTNER
P +1 650 463 5367

Related Services

Data Privacy

Featured Insights

CLIENT NEWS

Anduril Announces Acquisition of Klas to Advance Tactical Edge Computing and Communications

FIRM NEWS

Gunderson Dettmer Commemorates 2025 Asian American and Pacific Islander Heritage (AAPI) Month

CLIENT NEWS

Prosus Leads US$7.25M Financing of Zapia

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Latin American Fintech Clara Announces $80 Million Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

© 2025 Gunderson Dettmer; all rights reserved.