SDG
[ technology + passion ] – risk

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com

# The SHIELD Act: What Your Security Team Needs to Know—and Do

EVELIN BIRO

New York's SHIELD Act took effect on **March 21, 2020** and, in comparison with the GDPR sensation and California's follow-up, this act didn't generate too much fuss. In short, the people of New York decided to protect their data by updating the existing general business law with requirements for everyone who uses their private information.

More specifically, the state of New York enacted the "Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)." This Act updated the heading of article 39-F of general business law to "Notification of Unauthorized Acquisition of Private Information; Data Security Protections," updated the §899-aa and added a new paragraph, §899-bb.

This Act applies to any person or business that "owns or licenses computerized data which includes private information" of New York state residents, regardless of the business location.

The major highlights of the Act are:

1. The "Private Information" definition has been updated
2. The "Breach of the security of the system" definition has been updated
3. Compliance with certain regulations can be used as a proxy for SHIELD compliance
4. List of administrative, technical, and physical security requirements

Nothing in this law is unreasonable. It just requires reading, thinking, talking to a privacy lawyer, documenting, and taking action.

## A Few Steps to Get You Started

### 1. The "Private Information" Definition

The law provides three structures:

- Personal information: name, number, personal mark, etc.
- Data elements: SSN, financial with (or without) access numbers, biometric, etc.

- Private information: a combination of the previous two when either is unencrypted, or the encryption key has been accessed or acquired.

**CHAT WITH A LAWYER:** Facebook, LinkedIn, and Twitter are not government records and the "etc."-s above must be defined.

**OPPORTUNITY:** Revisit and update your data classification structure. If you don't have one, now is the time to build it. It is extremely useful and makes everyone's life much easier. However, don't make it so complicated that only your lawyer can understand it. Data classification is NOT for legal professionals; it is for people who do not want to deal with anything more than one if-then-else statement.

## 2. The "Breach of the Security of the System" Definition

This definition did not change much from its original form, other than for "ACCESS" and "PRIVATE." It still means that a breach is an access or acquisition of private information that was unauthorized or without a valid authorization.

The variables for a business to consider when deciding if an incident is a breach remain fairly informative. For example, if "...information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person," it is safe to conclude the incident is a breach.

The new part for security teams to note is that once the notice of the breach is made due to the requirements of other regulations (i.e. GLB, HIPAA/HITECH, 23 YNCRR 500, and other NY and federal laws), no additional notice to affected people is needed. However, notice to the state attorney general, the Department of State and the state policy, and consumer reporting agencies is still required.

**CHAT WITH A LAWYER:** Breach notification requirements are detailed in the law, addressing who, how, when and what. Every organization must detail processes and procedures per their circumstance and risk tolerance—including what *"the most expedient time," "unreasonable delay"* and *"any measures necessary"* mean.

**OPPORTUNITY:** Revisit and update your incident response plan. Ensure appropriate reporting, triage, evaluation, prioritization, escalation, containment, and remediation practices, along with proper root-cause analysis and corrective action. Detail incident classification and timeframe and an escalation path that includes CIO/CISO, legal, and communication representatives. Don't forget to outline a communication plan for informing asset owners and supervisory authorities and approving media and information sharing. Test it.

While the SHIELD Act has not made the same waves the GDPR and the California Privacy Act have, it is still important to be aware of its impacts. Subtle changes to rules and regulations can have a significant effect on the way organizations must respond to data breaches, and education is critical to moving forward successfully. For example, certain regulations can serve as a proxy for SHIELD compliance. Consider these practical applications of the SHIELD Act:

### 1. Compliance Proxy

The new section added to the GLB is §899-bb: "Data Security Protections." It recognizes compliance with the following regulations as a proxy:

- **GLB:** Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809)
- **HIPAA & HITECH:** Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), and the Health Information Technology for Economic and Clinical Health Act
- **23 NYCRR 500:** Part 500 of Title 23 of the official compilation of codes, rules and regulations of the state of New York, "Cybersecurity Requirements for Financial Services"
- **Any other data security rules and regulations** of the federal or New York state government

Essentially, your organization may already comply with the SHIELD Act—even if you have not taken explicit steps toward adhering to the new regulations. If you already comply with HIPAA, for example, there is a good chance that you also comply with the SHIELD Act.

### 2. Security Requirements

If your business does not have to comply with any of the aforementioned regulations, this Act provides a list of "reasonable security requirements" that must be implemented and maintained to "protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."

An organization will be deemed compliant if a data security program includes the following:

- **"Administrative Safeguards"**
  - designates one or more employees to coordinate the security program;
  - identifies reasonably foreseeable internal and external risks;
  - assesses the sufficiency of safeguards in place to control the identified risks;
  - trains and manages employees in the security program practices and procedures;
  - selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
  - adjusts the security program in light of business changes or new circumstances
- **"Technical Safeguards"**
  - assesses risks in network and software design;
  - assesses risks in information processing, transmission and storage
  - detects, prevents and responds to attacks or system failures; and
  - regularly tests and monitors the effectiveness of key controls, systems and procedures
- **"Physical Safeguards"**
  - assesses risks of information storage and disposal;
  - detects, prevents and responds to intrusions;
  - protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

- disposes 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.

Small organizations (< 50 people, < $3MM gross; <$5MM assets) are also required to comply with the Act by demonstrating reasonable administrative, technical and physical safeguards appropriate for the size and complexity of their business.

# Conclusion

The SHIELD Act is applicable to everyone who uses private information of New York residents, regardless of their size or physical location. Even third parties that indirectly use private information are obligated to comply. Organizations may use their compliance with other regulations (e.g. GLB, HIPAA) as proxy, assuming all security's administrative, technical and physical safeguards are in place.

Does your organization comply with the latest rules and regulations? At SDG, we have more than 25 years of experience in helping our clients eliminate their risks to critical corporate information and assets—and stay compliant with a multitude of regulations. To find out what we can do for your company, contact our team today.

# About Evelin Biro

As Principal Advisor and Practice Leader for SDG's Risk Management Practice, Evelin engages with clients to help design effective and organizationally tuned governance, risk management, compliance and data privacy programs. She advises IT and security leaders on how to position their programs in a strategic and business relevant way.

SDG

[ technology + passion ] – risk


- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com