Lawyers Alliance FOR NEW YORK
Connecting Lawyers, Nonprofits, and Communities

Updated August 14, 2025

New York's Data Protection and Breach Notification Laws

The Stop Hacks and Improve Electronic Data Security Act (SHIELD Act or the Act), which was signed into law in July 2019 (and amended in 2024), overhauled New York State's data breach notification framework and strengthened New York's data security framework. The SHIELD Act amended New York's 2005 Information Security Breach and Notification Act to bolster New York's data security laws and broadened both the definition of data breach and the scope of protective measures organizations must take.[1]

The SHIELD Act has two key components:

- Breach notification requirements that define when and how organizations must report incidents and what information must be protected, and
- "Reasonable safeguard" obligations that require covered entities to take steps to protect private information.[2]

This Legal Alert will provide information for nonprofits who may be subject to the SHIELD Act.

The SHIELD Act: Nonprofit Compliance

Even if your organization doesn't use or sell any personal data, the SHIELD Act likely still applies to your nonprofit. The SHIELD Act applies to any organization, including a nonprofit organization regardless of location or nonprofit status, that has received, collected, stored, or processed the computerized private information of a New York resident (even if unknowingly or unintentionally). Your nonprofit organization does not need to be selling or using that private information in any particular way to be covered under the Act. If you access the personal information of clients or even your employees who are New York residents, then the SHIELD Act likely applies to your organization.

A nonprofit should take steps to ensure that either (a) it does not have any New Yorker's private information, or (b) that it is compliant with the SHIELD Act requirements.[3] Nonprofits should review and update their data privacy policies to reflect the SHIELD Act's definitions of personal and private information, and ensure they are complying with proper data breach notification protocols. In addition, nonprofits deemed to be a "small business" under the Act should assess whether the organization

[1] N.Y. Gen. Bus. Law §§ 899-aa, 899-bb.

[2] As "reasonableness" is a facts and circumstances-influenced determination, it can be helpful to look to Attorney General guidance. *See* https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act#:~:text=Reasonable%20physical%20safeguards%20include%3A,destruction%20or%20disposal%20of%20information.

[3] "The term 'personal information,' upon which private information is largely based, means any information concerning a natural person …. Employees are natural persons and, if they are New York residents, likely will be protected by the SHIELD Act." Joseph J. Lazzarotti et al., New York SHIELD Act FAQs (March 11, 2020), https://natlawreview.com/article/new-york-shield-act-faqs.

meets the "reasonable safeguards" requirements discussed in more detail below.[4] All other nonprofits should confirm that they are implementing proper administrative, technical, and physical safeguards.[5]

Data Protection and Breach Notification Definitions

Covered organizations must ensure their data protection policies appropriately describe what constitutes protected private data and a breach of such data, as broadened by the relevant definitions of the SHIELD Act:

Breaches of Protected Data

Under the SHIELD Act, a data breach includes any unauthorized *access* to protected information. Prior to the SHIELD Act, only the actual *acquisition* of such information by an unauthorized person was considered a breach.[6] In determining whether a breach has occurred, covered entities may take into consideration factors such as whether the information has been viewed, communicated with, used, or altered by such unauthorized person. This means that, for example, if an employee falls for a phishing scam, even if your organization can show that no personal data was stolen, it could be considered a breach under the law.

Protected Data

New York requires protection of personal information and private information. The SHIELD Act defines these types of information as follows:

Personal information is any information from which you could personally identify an individual. It includes "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."[7]

Private information is a username or email address in combination with a password or security question and answer that would permit access to an account, or any personal information (as defined above) in combination with one or more of the corresponding individual's:

- Social Security number;
- Driver's license number or non-driver ID card number;
- Financial account, credit card, or debit card number, if such number could be used to access financial account without additional identifying information, security code, or password;
- Biometric information; or
- Username or email address and password credentials.[8]

The definition of private information does not include information that has been encrypted, so long as the encryption key has not also been accessed or acquired, and does not include information that is publicly available.

[4] N.Y. Gen. Bus. Law § 899-bb(2)(c).
[5] N.Y. Gen. Bus. Law § 899-bb(2)
[6] Italicized language refers to the changes made by the SHIELD Act.
[7] N.Y. Gen. Bus. Law § 899-aa(1)(a).
[8] N.Y. Gen. Bus. Law § 899-aa(1)(b).

Breach Notification Requirements

Covered organizations must comply with breach notification requirements under the SHIELD Act. In general, the Act requires that organizations inform affected consumers upon discovery of a security breach of its computer data system that affects protected information. In December 2024, an amendment took effect requiring organizations subject to the SHIELD Act to notify affected New York residents within 30 days of discovery of the breach.[9] However, notification is not required in every instance. Under the Act, organizations may evaluate data breaches based on a standard of harm. In particular, an organization would only be required to provide notice of a breach if the exposure is reasonably likely to result in misuse of the information or cause financial or emotional harm. Notification is also not required if the information was exposed inadvertently by a person who was authorized to access such information.[10]

If the organization determines that notification is required under the Act, it must provide the Attorney General, Department of State, and state police with a copy of the template notice that it sends to affected parties. A single submission of a breach form through the Attorney General's portal for breach reporting is sufficient for these purposes.[11] Per the 2024 amendment, organizations subject to regulation by the New York Department of Financial Services (DFS) must report breaches to the DFS as well.[12]

Best Practice Tip: Even when notification is not required under the Act, consider proactively informing consumers and advising them on protective steps. Organizations that have experienced a breach should reassure consumers that it is taking steps to contain the breach and advise them of any actions they can take to protect themselves, such as changing their password on relevant accounts.

Reasonable Safeguards for Nonprofit Organizations

The SHIELD Act also requires all covered organizations to implement reasonable safeguards to protect private information. The Act distinguishes between small businesses and all other businesses with respect to the requisite safeguards.

"Small businesses" must implement "reasonable administrative, technical, and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects

[9] N.Y. Senate Bill 2659, https://legiscan.com/NY/text/S02659/2023; N.Y. Gen. Bus. Law § 899-aa(3).
[10] N.Y. Gen. Bus. Law § 899-aa(2)(a). If your nonprofit believes the disclosure was inadvertent and does not pose a risk of harm, the nonprofit must document the determination in writing and maintain that documentation for at least five years. If the inadvertent disclosure affects over 500 New York residents, the nonprofit must provide the written determination to the state attorney general within 10 days after the determination.
[11] See https://formsnym.ag.ny.gov/OAGOnlineSubmissionForm/faces/OAGSBHome.
[12] N.Y. Senate Bill 2659, https://legiscan.com/NY/text/S02659/2023. See also Ashden Fein, Micaela McMurrough, Caleb Skeath, & Moriah Daugherty, New York Adopts Amendment to the State Data Breach Notification Law (January 7, 2025), https://www.insideprivacy.com/cybersecurity-2/new-york-adopts-amendment-to-the-state-data-breach-notification-law/.

from or about consumers."[13] An organization is a "small business" if it satisfies *one* of the following qualifications:

1. Has fewer than 50 employees;
2. Has less than $3 million in gross annual revenue in each of the last three fiscal years; *or*
3. Has less than $5 million in year-end total assets.[14]

All other organizations must implement more comprehensive data security programs in three key categories:

1. Administrative safeguards, such as the identification of employees to coordinate security programs, training of employees, assessment of potential risks and safeguards, and selection of outside service providers;
2. Technical safeguards, such as the assessment of risks in networks and software, information processing, detection, prevention and responsiveness to cyber threats, and monitoring of key controls, systems and procedures; and
3. Physical safeguards, such as adequate information storage and disposal processes, and detection and prevention of intrusions and unauthorized access.[15]

Compliance with New York's Data Protection and Breach Notification Laws

Determining what you need to do to comply with the Act can be a challenging question, and it depends on what you do with the data you collect, how it is collected, and how it is stored. If you believe that the Act applies to your organization and are concerned that you may have to take additional steps to come into compliance, we recommend that you consult with legal counsel for an analysis of risks and potential gaps that may exist.

Some steps that may need to be taken immediately depending on your circumstances are:

- Reviewing existing internal data protection policies to ensure appropriate coverage of protected information and breach notification requirements;
- Reviewing existing operating system security and third-party vendor platforms being used;
- Rolling out training for employees related to data privacy and security;
- Refreshing privacy policy and data use disclosures; and
- Developing compliant breach alert and reporting controls.

Non-Compliance Penalties: Failure to comply with the Act can bring significant penalties, making it important to know if your organization is compliant. The New York Attorney General can bring suit and

[13] N.Y. Gen. Bus. Law § 899-bb(2)(c). For one possible method to assess and demonstrate reasonableness, see John Banghart et al., Demonstrating a Reasonable Cybersecurity Program Through a Strategic Risk Assessment (Nov. 21, 2019), https://www.venable.com/insights/publications/2019/11/demonstrating-a-reasonable-cybersecurity-program.

[14] N.Y. Gen. Bus. Law § 899-bb(1)(c).

[15] N.Y. Gen. Bus. Law § 899-bb(2).

impose a fine of $5,000 *per violation* for failure to maintain reasonable safeguards.[16] Failure to provide notice of a breach that provided access to private information could result in a penalty of up to $20 per instance of failed notification, up to $250,000.

Differentiating the SHIELD Act from Other Privacy Frameworks

There is significant crossover between data protection and privacy acts that have been enacted around the world in the last decade, which is useful in making compliance easier. For example, the European Union's General Data Protection Regulation (GDPR)[17] and the SHIELD Act both have strict provisions about data breach notifications. However, GDPR and the SHIELD Act have different deadlines to notify affected people about a breach, definitions of a breach, and data protection requirements.[18] Such differences make it important for your organization to ensure that it is complying with specific SHIELD Act requirements, even if it already complies with other data protection laws.

An organization is deemed to be in compliance with the data protection policy requirements of the SHIELD Act if the business is regulated by and in compliance with:

- The Gramm-Leach-Bliley Act (covering companies that offer consumers financial products or services like loans, financial or investment advice, or insurance);
- The Health Insurance Portability and Accountability Act (HIPAA);
- The New York State Department of Financial Services' Cybersecurity Regulation under 23 NYCRR 500;[19] or
- "Any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government."[20]

Note, however, that most nonprofits will not fall under this regulated entity exemption to the SHIELD Act, so it is advisable to consult with legal counsel before presuming that this applies to you.

***

This alert is meant to provide general information only, not legal advice. If you have any questions about this alert please contact Ciarra Chavarria at cchavarria@lawyersalliance.org, or visit our website at www.lawyersalliance.org for further information.

---

[16] As an example, hackers gained access to sensitive emails through EyeMed's email account, which exposed protected personal data of its customers. The Attorney General investigated EyeMed's cybersecurity practices and determined that EyeMed was in violation of the SHIELD Act. EyeMed eventually reached settlement with New York State for a large fine plus a requirement that EyeMed implement a number of additional safeguards in connection with consumer personal data. See https://ag.ny.gov/press-release/2022/attorney-general-james-announces-600000-agreement-eyemed-after-2020-data-breach.

[17] See Lawyers Alliance, "The European Union's General Data Protection Regulation: What Nonprofits Need to Know" (Updated August 2025), www.lawyersalliance.org/userFiles/uploads/legal_alerts/GDPR_Legal_Alert.pdf.

[18] The organization has 72 hours after discovery of breach. See GDPR Art. 33, https://gdpr-info.eu/art-33-gdpr/.

[19] Entities covered by 23 NYCRR 500 are generally for-profit entities, like state-chartered banks, credit unions and insurance companies. See https://www.dfs.ny.gov/industry_guidance/cybersecurity.

[20] However, even regulated entities are not exempted from the data breach notification requirements of the Act, specifically, the requirement to notify the attorney general, department of state and state police and provide a template of the notice sent to affected persons. N.Y. Gen. Bus. Law § 899-bb(1)(a)(iv).

For her assistance in preparing this Legal Alert, Lawyers Alliance would like to thank Allison Shapiro, extern attorney from Skadden, Arps, Slate, Meagher & Flom.

Lawyers Alliance for New York is the leading provider of business and transactional legal services for nonprofit organizations and social enterprises that are improving the quality of life in New York City neighborhoods. Our network of pro bono lawyers from law firms and corporations and staff of experienced attorneys collaborate to deliver expert corporate, tax, real estate, employment, intellectual property, and other legal services to community organizations. By connecting lawyers, nonprofits, and communities, Lawyers Alliance for New York helps nonprofits to develop and provide housing, stimulate economic opportunity, improve urban health and education, promote community arts, and operate and advocate for vital programs that benefit low-income New Yorkers of all ages.