Lawyers Alliance FOR NEW YORK 1969 50 2019
Connecting Lawyers, Nonprofits, and Communities

December 19, 2019

Legal Alert: New York's Amendments to Data Protection and Breach Notification Laws

The Stop Hacks and Improve Electronic Data Security Act (SHIELD Act or the Act), effective as of October 23, 2019, amends New York State's data breach notification laws. The SHIELD Act has two key components: the first amends breach notification requirements and updates the definitions of what information must be protected, and the second adds new measures and requirements for safeguards to data security that covered entities must put into place (by March 21, 2020). The SHIELD Act also broadens the number of organizations that are covered, no longer just applying to entities conducting business in New York but to all entities (including nonprofits) that have collected, received, or stored a New York resident's private information. SHIELD Act Timetable for affected nonprofits:

by 10/23/19 Update data privacy policies to cover broader definitions of personal and private information.

Update data breach notification protocols.

by 03/21/20 "Small business" nonprofits, assess whether the organization meets the "reasonable safeguards" requirements.[i]

All other nonprofits implement to administrative, technical and physical safeguards.

1. My organization doesn't use or sell any personal data. Does the SHIELD Act apply to us?

The SHIELD Act applies to any organization, including a nonprofit organization, anywhere, that has received, collected, stored, or processed the computerized private information of a New York resident. Your nonprofit organization does not need to be using that private information in any particular way to be covered under the broad umbrella of the Act.

2. What does the SHIELD Act require?

The SHIELD Act makes several updates to the current data protection laws.

- Covered organizations must update their current data protection policies to take into account broader definitions of:
  - protected information – this is discussed in question 3 below.
  - what constitutes a data breach: a data breach now includes unauthorized *access* to protected information. Prior to the update, only the actual *acquisition* of such information by an unauthorized person was considered a breach. In determining whether protected information has been accessed, covered entities may take into consideration factors such as whether the information has been viewed, communicated with, used, or altered by such unauthorized person.

- Covered organizations must comply with an updated breach notification policy. One of the key changes to this policy is that organizations may now evaluate data breaches based on a standard of harm. In other words, an organization would not be required to provide notice of a breach if the exposure would not likely lead to misuse of the information, or financial or emotional harm.

When an organization determines that it is necessary to give notice of a data breach, however, it must now also provide the attorney general, department of state, and state police with a copy of the template notice it sends to affected parties.

- Covered organizations must implement certain data protection safeguards.
    - "Smaller 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 from or about consumers."[ii] While the Act is effective as of October 23, 2019, organizations have until March 21, 2020 to implement these safeguards.

      An organization is a "small business" if it satisfies *one* of the following qualifications:

      (i) has fewer than 50 employees; or
      (ii) has less than $3 million in gross annual revenue in each of the last three fiscal years; *or*
      (iii) has less than $5 million in year-end total assets.[iii]

    - All other organizations must implement more comprehensive data security programs by March 21, 2020 in three key categories:
      (i) Administrative safeguards, including the identification of employees to coordinate security programs, training of employees, assessment of potential risks and safeguards, and selection of outside service providers.
      (ii) Technical safeguards, including assessment of risks in networks and software, information processing, detection, prevention and responsiveness to cyber threats, and monitoring of key controls, systems and procedures.
      (iii) Physical safeguards, such as adequate information storage and disposal processes, and detection and prevention of intrusions and unauthorized access.

3. What types of information does the SHIELD Act cover?

The SHIELD Act requires protection of personal information and private information. As of October 23, 2019, the definitions for these types of information have been updated as follows (italicized language is new):

Personal information under the SHIELD Act is defined as 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."

Private information under the SHIELD Act is defined as 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;

- *Account number, credit or debit card number, if such number could be used to access financial account without additional identifying information, security code or password*; or
- *Biometric information.*

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. If my organization does not operate in New York, should I care about the SHIELD Act?

Yes. The Act applies to any entity with private information about a New York resident, regardless of where the entity does business or operates. Even if your organization does not operate in New York, you may very well, even unknowingly, have a New York resident's private information and therefore should take steps to ensure that either (a) you do not have any New Yorker's private information or (b) that you are compliant with the SHIELD Act requirements.

5. I already comply with other online data regulations; how is the SHIELD Act different?

There is a lot of crossover between data protection and privacy acts that have recently been enacted around the world, which is useful in making compliance easier. For example, the EU's General Data Protection Regulation (GDPR)[iv] 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. 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 will be 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),
- HIPAA
- the New York State Department of Financial Services' Cybersecurity Regulation under 23 NYCRR 500,[v] 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."[vi]

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.

6. If the SHIELD Act does apply to my organization, what steps do we need to take to comply?

Determining what you need to do to comply with the Act can be a challenging question, depending on what you do with 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 new steps to come into compliance, we recommend that you consult with legal counsel for an analysis of risks and potential gaps that may currently exist.

Some steps that may need to be taken by at least March 21, 2020 depending on your circumstances are:

- Review existing internal data protection policies and update definitions of protected information and breach notification policies;
- Review existing operating system security and third-party vendor platforms being used;
- Roll out training for employees related to data privacy and security;
- Refresh privacy policy and data use disclosures;
- Develop compliant breach alert and reporting controls.

7. Are there any penalties for noncompliance with the SHIELD Act?

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 impose a fine of $5,000 per violation. A failure to provide notice of a breach that provided access to private information could result in a penalty of the greater of $5,000 or $20 per instance of failed notification, up to $250,000.

Additional new regulations to look out for:

The California legislature recently signed into law the California Consumer Protection Act (CCPA), effective January 1, 2020.[vii] Unlike the SHIELD Act, the CCPA specifically only directly regulates for-profit businesses. However, a nonprofit will have to become CCPA compliant if it is controlled by a for-profit parent or controls a for-profit subsidiary that meets one of the following three criteria: (1) has $25 million in annual gross revenues; (2) has obtained the personal information of 50,000 California residents, households or devices in a year; or (3) at least 50% of their annual revenue is generated from selling California residents' personal information.

This alert is meant to provide general information only, not legal advice. If you have any questions about this alert please contact Senior Policy Counsel Laura Abel at (212) 219-1800 ext. 283 or visit our website at www.lawyersalliance.org for further information.

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.

---

[i] As "reasonableness" is a facts and circumstances-influenced determination, it can be helpful to look to the regulatory guidance and enforcement actions and statements from standards-setting bodies to help define what constitutes reasonable security practices, e.g., the Center for Internet Security's Twenty Critical Security Controls, https://www.cisecurity.org/controls/cis-controls-list/.

[ii] 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.

[iii] N.Y. Gen. Bus. Law § 899-aa.

[iv] *See* Lawyers Alliance, "Legal Alert: Should My Nonprofit Organization Be Concerned about the European Union's New Data Law?" (Aug. 2018), https://lawyersalliance.org/userFiles/uploads/legal_alerts/GDPR_Legal_Alert_August_2018_FINAL_UPDATE.pdf.

[v] 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/docs/legal/regulations/adoptions/dfsrf500txt.pdf

[vi] 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.

[vii] *See* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.