SOLUTION OVERVIEW

How Spirion Advances Compliance with New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)

Effective on March 21, 2020, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)[1] offers significant protection for the private information of New York residents. Highlights of the Act include:

- An expanded definition of "private information";
- Applicability to any person or entity that accesses the private information of a New York resident — acquiring the information is not necessary, nor is conducting business in the state;
- Breach notification "in the most expedient time possible and without unreasonable delay" to affected parties and several New York law enforcement agencies; and
- Mandate to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information including secure disposal of data.

For violations of the breach notification mandate, the New York Attorney General may bring actions for civil penalties of (1) up to actual damages incurred by residents for violations that are based on negligence; and (2) up to $5,000 per violation (with a $250,000 limit) for violations that are "knowing" or "reckless" (either is a higher standard). For violations of the "reasonable safeguards" requirement, the Attorney General may seek damages of up to $5,000 per violation.

[1] S. 5575-B; amends N.Y. Gen. Bus. Law § 899-aa and N.Y. State Tech. Law § 208. Adds Gen. Bus. Law § 899-bb.

Stated Requirement	How Spirion Advances CCPA Compliance
Identify "private information"	The SHIELD Act includes the following as private information: 1. Social security number; 2. Driver's license number or non-driver identification card number; 3. Account number, credit or debit card number, in combination with any required security code, access code, password, or other information; 4. Account number, credit, or debit card number; 5. Biometric information; or 6. User name or e-mail address in combination with a password or security question and answer. Featuring a proprietary algorithm, Spirion's AnyFind® technology identifies, remotely or locally, both structured and unstructured personal data throughout your organization in share files, emails, websites, databases, Microsoft SharePoint, and cloud storage, all with the industry's highest precision. With Spirion, you'll locate hard-to-find data such as machine-readable data, national ID numbers, identifiers tied to mobile devices and applications, and references to data that is unique to the company.

Stated Requirement	How Spirion Advances CCPA Compliance
Breach notification	When unauthorized access to private information is detected, the owner or licensee of the information involved must notify: • Affected New York residents "in the most expedient time possible and without unreasonable delay"; • The state attorney general, the department of state, and the division of state police "as to the timing content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons"; and • Consumer reporting agencies. Third-party service providers must also notify their customers immediately when unauthorized access is detected. Spirion's AnyFind technology enables you to develop a comprehensive data inventory of private information. The inventory becomes a "single source of truth" for determining what private information was implicated by the breach and enables you to rapidly develop accurate.
Information security	The Act's requirement to provide "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information" is similar to that of the NYCRR Part 500, GDPR, and many other data protection regulations. In particular, the Act cites the need for technical safeguards. Spirion takes a proactive approach to this using Sensitive Data Watcher™. Sensitive Data Watcher continuously monitors a business' information ecosystem for new data and when a file is created, copied, edited, detached from an email, extracted from an archive, retrieved from the cloud or enterprise storage, or otherwise modified, it is instantly searched, automatically classified, and reported upon. From there, protection options for that data can be automated by the Spirion Workflow and Classification engine. By applying business requirements to the matched data and associated metadata, Spirion can persistently classify (tag) files and perform remediation actions on them, including encrypting, shredding, redacting certain elements, or quarantining files to a more secure location. Data protection staff can set triggers that automatically notify them via email of policy violations for immediate response. Spirion also offers the option to invoke a script, enabling allied systems to assist in the remediation process. You can also include end users and data owners in these efforts by empowering them to perform remediation on an ad hoc basis.
Secure disposal of private information	Disposal of private information must both be permanent and provable. Spirion's Workflow and Classification engine enables automated deletion of files containing private information or redaction of personal data elements according to criteria you set. Associated reporting provides compelling evidence of compliance with the Act's secure disposal requirement.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to public sector. Visit us at **spirion.com**