STATE OF NEW YORK

1961--A

2025-2026 Regular Sessions

IN SENATE

January 14, 2025

Introduced by Sen. GONZALEZ -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- recommitted to the Committee on Internet and Technology in accordance with Senate Rule 6, sec. 8 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the state technology law, in relation to establishing the "secure our data act"

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "secure our data act".

§ 2. Legislative intent. The legislature finds that information technology attacks and breaches have compromised governmental networks and the electronically stored personal information of countless people statewide and nationwide. State entities often receive such personal information from various sources, including the data subjects themselves, other state entities, and the federal government. Additionally, state entities use such personal information to make determinations regarding data subjects. New Yorkers deserve to have their personal information in the possession of a state entity stored in a manner that will withstand any attempt by a bad actor to access, alter, or prohibit access to such information.

Therefore, the legislature enacts the secure our data act, which will require state entities to employ adequate practices and systems to protect the personal information from any unauthorized acquisition, access, alteration or change in access.

§ 3. The state technology law is amended by adding a new section 211 to read as follows:

§ 211. Cybersecurity protection. 1. Definitions. For purposes of this section, the following terms shall have the following meanings:

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD05506-02-6

(a) "Breach of the security of the system" means (i) unauthorized exfiltration, acquisition, or acquisition without valid authorization, of computerized information which compromises the security, confidentiality, or integrity of state entity-maintained personal information, (ii) unauthorized access, or access without valid authorization, to state entity-maintained personal information or to an information system used for personal information, or (iii) unauthorized modification of the access permissions, including through the use of encryption, to an information system used for personal information. "Breach of the security of the system" does not include good faith acquisition of or access to personal information, or access to an information system by an employee or agent of a state entity for the purposes of the state entity; provided that the private information or information system is not used in an unauthorized manner, accessed for an unlawful or inappropriate purpose, modified to change access permissions without authorization, or subject to unauthorized disclosure. In determining whether state entity-maintained personal information or an information system used for personal information has been exfiltrated, acquired, accessed, or experienced a change in access permissions without authorization or without valid authorization, such state entity may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;

(2) indications that the information has been downloaded or copied;

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(4) indications that the information or information system was accessed without authorization or without valid authorization, including but not limited to data in information system access logs, changes modifying access to the information or information system, modification or deletion of stored information, injecting or installing malicious code on the information system, or unauthorized encryption of stored information.

(b) "Data subject" means the person who is the subject of the personal information.

(c) "Data validation" means ensuring the accuracy, quality, and validity of source data before using, importing, saving, storing, or otherwise processing data.

(d) "Immutable" means data that is stored unchanged over time or unable to be changed. For the purposes of backups, "immutable" shall mean that, once ingested, no external or internal operation can modify the data and must never be available in a read/write state to the client. "Immutable" shall specifically apply to the characteristics and attributes of a backup system's file system and may not be applied to temporary systems state, time-bound or expiring configurations, or temporary conditions created by a physical air gap as is implemented in most legacy systems, provided that immutable backups must be capable of deletion and replacement, as applicable, in accordance with the data retention and deletion policy governing the data. An immutable file system must demonstrate characteristics that do not permit the editing or changing of any data backed up to provide agencies with complete recovery capabilities.

(e) "Information system" means any good, service or a combination thereof, used by any computer, cloud service, or interconnected system

that is maintained for or used by a state entity in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or voice including, but not limited to, hardware, software, information appliances, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically and electronically collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, coverage, interface, switch, or disseminate data or information of any kind or form.

(f) "Mission critical" means information or information systems that are essential to the functioning of the state entity.

(g) "Segmented storage" means the method of data storage whereby (i) information is partitioned or separated, with overlapping or non-overlapping protection, and (ii) such individual partitioned or separated sets of information are stored in multiple physically or logically distinct secure locations.

(h) "State entity-maintained personal information" means personal information stored by a state entity that was generated by a state entity or provided to the state entity by the data subject, a state entity, a federal governmental entity, or any other third-party source. Such term shall also include personal information provided by an adverse party in the course of litigation or other adversarial proceeding.

(i) "State entity" means any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

(i) the judiciary; and

(ii) all cities, counties, municipalities, villages, towns, and other local agencies.

2. Data protection standards. (a) No later than one year after the effective date of this section, the director, in consultation with stakeholders and other interested parties, which shall include at least one public hearing, shall promulgate regulations that design and develop standards for:

(i) protection against breaches of the security of the system for mission critical information systems and for personal information used by such information systems;

(ii) data backup that includes;

(A) the creation of immutable backups of state entity-maintained personal information;

(B) through data validation techniques, the exclusion of unwanted data from such immutable backups, including but not limited to illegal content, corrupted data, malicious code, and content that breaches intellectual property protections;

(C) prohibitions on the use of such immutable backups except for conducting data validation and performing information system recovery; and

(D) storage of such immutable backups in segmented storage;

(iii) information system recovery that includes creating an identical copy of an immutable backup of state entity-maintained personal information in segmented storage for use when an information system has been adversely affected by a breach of the security of the system and requires restoration from one or more backups;

(iv) data retention and deletion policies specifying how long certain types of data shall be retained on information systems and as immutable

backups in segmented storage and when or under what circumstances such data shall be deleted; and

(v) annual workforce training regarding protection against breaches of the security of the system, as well as processes and procedures that should be followed in the event of a breach of the security of the system.

(b) Such regulations may be adopted on an emergency basis. If such regulations are adopted on an emergency basis, the office shall engage in the formal rulemaking procedure no later than the day immediately following the date that the office promulgated such regulations on an emergency basis. Provided that the office has commenced the formal rule-making process, the regulations adopted on an emergency basis may be renewed no more than two times.

3. Vulnerability assessments. Notwithstanding any provision of law to the contrary, each state entity shall engage in vulnerability testing of its information systems as follows:

(a) Beginning January first, two thousand twenty-seven and on a month-ly basis thereafter, each state entity shall perform, or cause to be performed, a vulnerability assessment of at least one mission critical information system ensuring that each mission critical system has under-gone a vulnerability assessment during the past year. A report detailing the vulnerability assessment methodology and findings shall be made available to the office for review no later than forty-five days after the testing has been completed.

(b) Beginning December first, two thousand twenty-seven, each state entity's entire information system shall undergo vulnerability testing. A report detailing the vulnerability assessment methodology and findings shall be made available to the office for review no later than forty-five days after such testing has been completed.

(c) The office shall assist state entities in complying with the provisions of this section.

4. Data and information system inventory. (a) No later than one year after the effective date of this section, each state entity shall create an inventory of the state entity-maintained personal information and the purpose or purposes for which such state entity-maintained personal information is maintained and used. The inventory shall include a list-ing of all types of state entity-maintained personal information, along with the source and the median age of such information.

(b) No later than one year after the effective date of this section, each state entity shall create an inventory of its information systems and the purpose or purposes for which each such information system is maintained and used. The inventory shall denote those information systems that are mission critical and those that use personal informa-tion, and whether the information system is protected by immutable back-ups and stored in a segmented manner.

(c) Notwithstanding paragraphs (a) and (b) of this subdivision, if a state entity has already completed a state entity-maintained personal information inventory or information systems inventory, such state enti-ty shall update the previously completed state entity-maintained personal information inventory or information system inventory no later than one year after the effective date of this section.

(d) Upon written request from the office, a state entity shall provide the office with either or both of the state entity-maintained personal information and information systems inventories required to be created or updated pursuant to this subdivision.

(e) Notwithstanding paragraph (d) of this subdivision, the state entity-maintained personal information and information systems inventories required to be created or updated pursuant to this subdivision shall be kept confidential and shall not be made available for disclosure or inspection under the state freedom of information law unless a subpoena or other court order directs the office or state entity to release such inventory or information from such inventory.

5. Incident management and recovery. (a) No later than eighteen months after the effective date of this section, each state entity shall have created an incident response plan for incidents involving a breach of the security of the system that render an information system or its data unavailable, and incidents involving a breach of the security of the system that result in the alteration or deletion of or unauthorized access to, personal information.

(b) Such incident response plan shall include a procedure for situations where information systems have been adversely affected by a breach of the security of the system, as well as a procedure for the storage of personal information and mission critical backups in segmented storage to ensure that such personal information and mission critical systems are protected by immutable backups.

(c) Beginning January first, two thousand twenty-nine and on an annual basis thereafter, each state entity shall complete at least one exercise of its incident response plan that includes copying the immutable personal information and mission critical applications from the segmented portion of the state entity's information system and using such copies in the state entity's restoration and recovery process. Upon completion of such exercise, the state entity shall document the incident response plan's successes and shortcomings in an incident response plan exercise report. Such incident response plan exercise report shall be kept confidential and shall not be made available for disclosure or inspection under the state freedom of information law unless a subpoena or other court order directs the state entity to release such inventory or information from such inventory.

6. No private right of action. Nothing set forth in this section shall be construed as creating or establishing a private cause of action.

§ 4. Severability. The provisions of this act shall be severable and if any portion thereof or the applicability thereof to any person or circumstances shall be held to be invalid, the remainder of this act and the application thereof shall not be affected thereby.

§ 5. This act shall take effect immediately.