

STATE OF NEW YORK

5007--B

Cal. No. 485

2023-2024 Regular Sessions

IN SENATE

February 21, 2023

Introduced by Sens. GONZALEZ, SALAZAR -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- reported favorably from said committee and committed to the Committee on Finance -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- recommitted to the Committee on Internet and Technology in accordance with Senate Rule 6, sec. 8 -- reported favorably from said committee and committed to the Committee on Finance -- reported favorably from said committee, ordered to first and second report, ordered to a third reading, amended and ordered reprinted, retaining its place in the order of third reading

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:

1 Section 1. This act shall be known and may be cited as the "secure our
2 data act".
3 § 2. Legislative intent. The legislature finds that ransomware and
4 other malware attacks have affected the electronically stored personal
5 information relating to thousands of people statewide and millions of
6 people nationwide. The legislature also finds that state entities
7 receive such personal information from various sources, including the
8 data subjects themselves, other state entities, and the federal govern-
9 ment. In addition, the legislature finds that state entities use such
10 personal information to make determinations regarding the data subjects.
11 The legislature further finds that New Yorkers deserve to have their
12 personal information that is in the possession of a state entity stored
13 in a manner that will withstand any attempt by ransomware and other
14 malware to alter, change, or encrypt such information.
15 Therefore, the legislature enacts the secure our data act which will
16 guarantee that state entities will employ the proper technology to

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

LBD09002-04-4

1 protect the personal information stored as backup information from any
2 unauthorized alteration or change.

3 § 3. The state technology law is amended by adding a new section 210
4 to read as follows:

5 § 210. Ransomware and other malware protection. 1. Definitions. For
6 purposes of this section, the following terms shall have the following
7 meanings:

8 (a) "Data subject" shall mean the person who is the subject of the
9 personal information.

10 (b) "Immutable" means data that is stored unchanged over time or
11 unable to be changed. For the purposes of backups, "immutable" shall
12 mean that, once ingested, no external or internal operation can modify
13 the data and must never be available in a read/write state to the
14 client. "Immutable" shall specifically apply to the characteristics and
15 attributes of a backup system's file system and may not be applied to
16 temporary systems state, time-bound or expiring configurations, or
17 temporary conditions created by a physical air gap as is implemented in
18 most legacy systems. An immutable file system must demonstrate charac-
19 teristics that do not permit the editing or changing of any data backed
20 up to provide agencies with complete recovery capabilities.

21 (c) "Information system" shall mean any good, service or a combination
22 thereof, used by any computer, cloud service, or interconnected system
23 that is maintained for or used by a state entity in the acquisition,
24 storage, manipulation, management, movement, control, display, switch-
25 ing, interchange, transmission, or reception of data or voice including,
26 but not limited to, hardware, software, information appliances, firm-
27 ware, programs, systems, networks, infrastructure, media, and related
28 material used to automatically and electronically collect, receive,
29 access, transmit, display, store, record, retrieve, analyze, evaluate,
30 process, classify, manipulate, manage, assimilate, control, communicate,
31 exchange, convert, coverage, interface, switch, or disseminate data of
32 any kind or form.

33 (d) "Maintained" shall mean personal information stored by a state
34 entity that was provided to the state entity by the data subject, a
35 state entity, or a federal governmental entity. Such term shall also
36 include personal information provided by an adverse party in the course
37 of litigation or other adversarial proceeding.

38 (e) "Malware" shall mean malicious code included in any application,
39 digital content, document, executable, firmware, payload, or software
40 for the purpose of performing or executing one or more unauthorized
41 processes designed to have an adverse impact on the availability, confi-
42 dentiality, or integrity of data stored in an information system.

43 (f) "Ransomware" shall mean any type of malware that uses encryption
44 technology to prevent users from accessing an information system or data
45 stored by such information system until a ransom is paid.

46 (g) "State entity" shall mean any state board, bureau, division,
47 committee, commission, council, department, public authority, public
48 benefit corporation, office or other governmental entity performing a
49 governmental or proprietary function for the state of New York, except:

50 (i) the judiciary; and

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

53 2. Data protection standards. (a) No later than one year after the
54 effective date of this section, the director, in consultation with
55 stakeholders and other interested parties, which shall include at least

1 one public hearing, shall promulgate regulations that design and develop
2 standards for:

3 (i) malware and ransomware protection for mission critical information
4 systems and for personal information used by such information systems;

5 (ii) data backup that includes the creation of immutable backups of
6 personal information maintained by the state entity and storage of such
7 backups in a segmented environment, including a segmented device;

8 (iii) information system recovery that includes creating an identical
9 copy of an immutable personal information backup maintained by or for
10 the state entity that was stored in a segmented environment or on a
11 segmented device for use when an information system has been adversely
12 affected by rent somewhere or other malware and requires restoration
13 from one or more backups; and

14 (iv) annual workforce training regarding protection from ransomware
15 and other malware, as well as processes and procedures that should be
16 followed in the event of a data incident involving ransomware or other
17 malware.

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

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

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

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

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

43 4. Data and information system inventory. (a) No later than one year
44 after the effective date of this section, each state entity shall create
45 an inventory of the data maintained by the state entity and the purpose
46 or purposes for which such data is maintained and used. The inventory
47 shall include a listing of all personal information maintained by the
48 state entity, along with the source and age of such information.

49 (b) No later than one year after the effective date of this section,
50 each state entity shall create an inventory of the information systems
51 maintained by or on behalf of the state entity and the purpose or
52 purposes for which each such information system is maintained and used.
53 The inventory shall denote those information systems that are mission
54 critical and those that use personal information, and whether the infor-
55 mation system is protected by immutable backups.

1 (c) Notwithstanding paragraphs (a) and (b) of this subdivision, if a
2 state entity has already completed a data inventory or information
3 systems inventory, such state entity shall update the previously
4 completed data inventory or information system inventory no later than
5 one year after the effective date of this section.

6 (d) Upon written request from the office, a state entity shall provide
7 the office with either or both of the inventories required to be created
8 or updated pursuant to this subdivision.

9 5. Incident management and recovery. (a) No later than eighteen months
10 after the effective date of this section, each state entity shall have
11 created an incident response plan for incidents involving ransomware or
12 other malware that renders an information system or its data unavail-
13 able, and incidents involving ransomware or other malware that result in
14 the alteration or deletion of or unauthorized access to, personal infor-
15 mation.

16 (b) Such incident response plan shall include a procedure for situ-
17 ations where production and non-segmented information systems have been
18 adversely affected by a data incident, as well as a procedure for the
19 storage of personal information and mission critical backups on a
20 segmented device or segmented portion of the state entity's information
21 system to ensure that such personal information and mission critical
22 systems are protected by immutable backups.

23 (c) Beginning January first, two thousand twenty-seven and on an annu-
24 al basis thereafter, each state entity shall complete at least one exer-
25 cise of its incident response plan that includes copying the immutable
26 personal information and mission critical applications from the
27 segmented portion of the state entity's information system and using
28 such copies in the state entity's restoration and recovery process. Upon
29 completion of such exercise, the state entity shall document the inci-
30 dent response plan's successes and shortcomings.

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

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

37 § 5. This act shall take effect immediately.