## STATE OF NEW YORK

5736

2023-2024 Regular Sessions

## IN ASSEMBLY

March 23, 2023

Introduced by M. of A. SOLAGES -- read once and referred to the Committee on Governmental Operations

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 ransomware and 3 4 other malware attacks have affected the electronically stored personal 5 information relating to thousands of people statewide and millions of people nationwide. The legislature also finds that state entities б 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 personal information to make determinations regarding the data subjects. 10 The legislature further finds that New Yorkers deserve to have their 11 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 17 protect the personal information stored as backup information from any 18 unauthorized alteration or change.

19 § 3. The state technology law is amended by adding a new section 210 20 to read as follows:

21 § 210. Ransomware and other malware protection. 1. Definitions. For 22 purposes of this section, the following terms shall have the following 23 meanings:

24 (a) "Data subject" shall mean the person who is the subject of the 25 personal information.

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

LBD09002-01-3

A. 5736

(b) "Immutable" means data that is stored unchanged over time or 1 unable to be changed. For the purposes of backups, "immutable" shall 2 mean that, once ingested, no external or internal operation can modify 3 4 the data and must never be available in a read/write state to the 5 client. "Immutable" shall specifically apply to the characteristics and 6 attributes of a backup system's file system and may not be applied to 7 temporary systems state, time-bound or expiring configurations, or temporary conditions created by a physical air gap as is implemented in 8 9 most legacy systems. An immutable file system must demonstrate charac-10 teristics that do not permit the editing or changing of any data backed 11 up to provide agencies with complete recovery capabilities. 12 (c) "Information system" shall mean any good, service or a combination thereof, used by any computer, cloud service, or interconnected system 13 14 that is maintained for or used by a state entity in the acquisition, 15 storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or voice including, 16 17 but not limited to, hardware, software, information appliances, firmware, programs, systems, networks, infrastructure, media, and related 18 material used to automatically and electronically collect, receive, 19 20 access, transmit, display, store, record, retrieve, analyze, evaluate, 21 process, classify, manipulate, manage, assimilate, control, communicate, 22 exchange, convert, coverage, interface, switch, or disseminate data of 23 any kind or form. (d) "Maintained" shall mean personal information stored by a state 24 25 entity that was provided to the state entity by the data subject, a state entity, or a federal governmental entity. Such term shall also 26 27 include personal information provided by an adverse party in the course 28 of litigation or other adversarial proceeding. 29 (e) "Malware" shall mean malicious code included in any application, 30 digital content, document, executable, firmware, payload, or software for the purpose of performing or executing one or more unauthorized 31 32 processes designed to have an adverse impact on the availability, confi-33 dentiality, or integrity of data stored in an information system. 34 (f) "Ransomware" shall mean any type of malware that uses encryption 35 technology to prevent users from accessing an information system or data 36 stored by such information system until a ransom is paid. 37 (g) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public 38 39 benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York or any of 40 41 its political subdivisions. 42 2. Data protection standards. (a) No later than one year after the 43 effective date of this section, the director, in consultation with 44 stakeholders and other interested parties, which shall include at least 45 one public hearing, shall promulgate regulations that design and develop 46 standards for: 47 (i) malware and ransomware protection for mission critical information 48 systems and for personal information used by such information systems; 49 (ii) data backup that includes the creation of immutable backups of personal information maintained by the state entity and storage of such 50 backups in a segmented environment, including a segmented device; 51 52 (iii) information system recovery that includes creating an identical copy of an immutable personal information backup maintained by or for 53 the state entity that was stored in a segmented environment or on a 54 segmented device for use when an information system has been adversely 55

2

A. 5736

1	affected by rent somewhere or other malware and requires restoration
2	from one or more backups; and
3	(iv) annual workforce training regarding protection from ransomware
4	and other malware, as well as processes and procedures that should be
5	followed in the event of a data incident involving ransomware or other
б	malware.
7	(b) Such regulations may be adopted on an emergency basis. If such
8	regulations are adopted on an emergency basis, the office shall engage
9	in the formal rulemaking procedure no later than the day immediately
10	following the date that the office promulgated such regulations on an
11	emergency basis. Provided that the office has commenced the formal rule-
12	making process, the regulations adopted on an emergency basis may be
13	renewed no more than two times.
$14^{13}$	3. Vulnerability assessments. Notwithstanding any provision of law to
15	the contrary, each state entity shall engage in vulnerability testing of
16	its information systems as follows:
17	
	(a) Beginning January first, two thousand twenty-four and on a monthly
18	basis thereafter, each state entity shall perform, or cause to be
19	performed, a vulnerability assessment of at least one mission critical
20	information system ensuring that each mission critical system has under-
21	gone a vulnerability assessment during the past year. A report detailing
22	the vulnerability assessment methodology and findings shall be made
23	available to the office for review no later than forty-five days after
24	the testing has been completed.
25	(b) Beginning December first, two thousand twenty-four, each state
26	entity's entire information system shall undergo vulnerability testing
27	conducted by an independent third party. A report detailing the vulner-
28	ability assessment methodology and findings shall be made available to
29	the office for review no later than forty-five days after such testing
30	has been completed.
31	(c) The office shall assist state entities in complying with the
32	provisions of this section.
33	4. Data and information system inventory. (a) No later than one year
34	after the effective date of this section, each state entity shall create
35	an inventory of the data maintained by the state entity and the purpose
36	or purposes for which such data is maintained and used. The inventory
37	shall include a listing of all personal information maintained by the
38	state entity, along with the source and age of such information.
39	(b) No later than one year after the effective date of this section,
40	each state entity shall create an inventory of the information systems
41	maintained by or on behalf of the state entity and the purpose or
42	purposes for which each such information system is maintained and used.
43	The inventory shall denote those information systems that are mission
44	critical and those that use personal information, and whether the infor-
45	mation system is protected by immutable backups.
46	(c) Notwithstanding paragraphs (a) and (b) of this subdivision, if a
47	state entity has already completed a data inventory or information
48	systems inventory, such state entity shall update the previously
49	completed data inventory or information system inventory no later than
50	one year after the effective date of this section.
51	(d) Upon written request from the office, a state entity shall provide
52	the office with either or both of the inventories required to be created
53	or updated pursuant to this subdivision.
54	5. Incident management and recovery. (a) No later than eighteen months
55	after the effective date of this section, each state entity shall have
56	created an incident response plan for incidents involving ransomware or

A. 5736

1	other malware that renders an information system or its data unavail-
2	able, and incidents involving ransomware or other malware that result in
3	the alteration or deletion of or unauthorized access to, personal infor-
4	mation.
5	(b) Such incident response plan shall include a procedure for situ-
б	ations where production and non-segmented information systems have been
7	adversely affected by a data incident, as well as a procedure for the
8	storage of personal information and mission critical backups on a
9	segmented device or segmented portion of the state entity's information
10	system to ensure that such personal information and mission critical
11	systems are protected by immutable backups.
12	(c) Beginning January first, two thousand twenty-six and on an annual
13	basis thereafter, each state entity shall complete at least one exercise
14	of its incident response plan that includes copying the immutable
15	personal information and mission critical applications from the
16	segmented portion of the state entity's information system and using
17	such copies in the state entity's restoration and recovery process. Upon
18	completion of such exercise, the state entity shall document the inci-
19	dent response plan's successes and shortcomings.
20	6. No private right of action. Nothing set forth in this section shall
21	be construed as creating or establishing a private cause of action.
22	§ 4. Severability. The provisions of this act shall be severable and
23	if any portion thereof or the applicability thereof to any person or
24	circumstances shall be held to be invalid, the remainder of this act and
25	the application thereof shall not be affected thereby.

26 § 5. This act shall take effect immediately.