# HB2871

LRB101 08512 JRG 53589 b

## 101ST GENERAL ASSEMBLY

## State of Illinois

## 2019 and 2020

### HB2871

by Rep. Celina Villanueva

## SYNOPSIS AS INTRODUCED:

New Act

Creates the Data Broker Registration Act. Requires a data broker to annually register with the Secretary of State. Defines "data broker" as a business or unit of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Provides registration requirements, the duties a data broker has to protect personally identifiable information, and the requirements for an information security program. Effective January 1, 2020.

LRB101 08512 JRG 53589 b

FISCAL NOTE ACT
MAY APPLY

A BILL FOR

AN ACT concerning regulation.

**Be it enacted by the People of the State of Illinois, represented in the General Assembly:**

Section 1. Short title. This Act may be cited as the Data Broker Registration Act.

Section 5. Definitions.

"Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(1) name;

(2) address;

(3) date of birth;

(4) place of birth;

(5) mother's maiden name;

(6) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(7) name or address of a member of the consumer's immediate family or household;

(8) social security number or other government-issued

identification number; or

(9) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

"Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

"Data broker" means a business or unit of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

"Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person. "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker if the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.

Section 10. Annual registration.

(a) Annually, on or before January 31 following a year in which a person meets the definition of "data broker", a data broker shall:

(1) register with the Secretary of State;

(2) pay a registration fee of $100; and

(3) provide the following information:

(A) the name and primary physical, email, and Internet addresses of the data broker;

(B) if the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:

(i) the method for requesting an opt-out;

(ii) if the opt-out applies to only certain activities or sales, which ones; and

(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) a statement whether the data broker implements a purchaser credentialing process;

(E) the number of data broker security breaches

that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

(G) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register under subsection (a) is liable to the State for:

(1) a civil penalty of $50 for each day, not to exceed a total of $10,000 for each year, it fails to register under this Section;

(2) an amount equal to the fees due under this Section during the period it failed to register under this Section; and

(3) other penalties imposed by law.

(c) The Attorney General may maintain an action in circuit court to collect the penalties imposed in this Section and to seek appropriate injunctive relief.

Section 15. Duty to protect personally identifiable

information.

(a) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(1) the size, scope, and type of business of the data broker obligated to safeguard the personally identifiable information under such comprehensive information security program;

(2) the amount of resources available to the data broker;

(3) the amount of stored data; and

(4) the need for security and confidentiality of personally identifiable information.

(b) A data broker subject to this Section shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker.

Section 20. Information security program; minimum features. A comprehensive information security program shall, at minimum, have the following features:

(1) designation of one or more employees to maintain

the program;

(2) identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) ongoing employee training, including training for temporary and contract employees;

(B) employee compliance with policies and procedures; and

(C) means for detecting and preventing security system failures;

(3) security policies for employees relating to the storage, access, and transportation of records containing personally identifiable information outside business premises;

(4) disciplinary measures for violations of the comprehensive information security program rules;

(5) measures that prevent terminated employees from accessing records containing personally identifiable information;

(6) supervision of service providers by:

(A) taking reasonable steps to select and retain third-party service providers that are capable of

maintaining appropriate security measures to protect personally identifiable information consistent with applicable law; and

(B) requiring third-party service providers by contract to implement and maintain appropriate security measures for personally identifiable information;

(7) reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in locked facilities, storage areas, or containers;

(8) regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information; and upgrading information safeguards as necessary to limit risks;

(9) regular review of the scope of the security measures:

(A) at least annually; or

(B) whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personally identifiable information; and

(10) documentation of responsive actions taken in connection with any incident involving a breach of

security; and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

Section 25. Information security program; computer system security requirements. A comprehensive information security program required by this Act shall, at minimum, and to the extent technically feasible, have the following elements:

(1) secure user authentication protocols, as follows:

(A) an authentication protocol that has the following features:

(i) control of user IDs and other identifiers;

(ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(iii) control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;

(iv) restricting access to only active users and active user accounts; and

(v) blocking access to user identification after multiple unsuccessful attempts to gain access; or

(B) an authentication protocol that provides a higher level of security than the features specified in subparagraph (A).

(2) secure access control measures that:

(A) restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and

(B) assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(3) encryption of all transmitted records and files containing personally identifiable information that will travel across public networks and encryption of all data containing personally identifiable information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(4) reasonable monitoring of systems for unauthorized use of or access to personally identifiable information;

(5) encryption of all personally identifiable information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(6) for files containing personally identifiable

information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security;

(7) reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

(8) education and training of employees on the proper use of the computer security system and the importance of personally identifiable information security.

Section 99. Effective date. This Act takes effect January 1, 2020.