By: Johnson, Menéndez S.B. No. 2105

(In the Senate - Filed March 9, 2023; March 21, 2023, read first time and referred to Committee on Business & Commerce; April 28, 2023, reported adversely, with favorable Committee Substitute by the following vote: Yeas 11, Nays 0; April 28, 2023, sent to printer.)

COMMITTEE VOTE

	Yea	Nay	Absent	PNV
Schwertner	X			
King	X			
Birdwell	X			
Campbell	X			
Creighton	X			
Johnson	X			
Kolkhorst	X			
Menéndez	X			
Middleton	X			
Nichols	X			
Zaffirini	X			

COMMITTEE SUBSTITUTE FOR S.B. No. 2105 By: Johnson

A BILL TO BE ENTITLED
AN ACT

relating to the registration of and certain other requirements relating to data brokers; providing a civil penalty and authorizing a fee.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subtitle A, Title 11, Business & Commerce Code, is amended by adding Chapter 509 to read as follows:

CHAPTER 509. DATA BROKERS

Sec. 509.001. DEFINITIONS. In this chapter:

(1) "Biometric data" means data generated by automatic measurements of an individual's biological patterns or characteristics, including fingerprint, voiceprint, retina or iris scan, information pertaining to an individual's DNA, or another unique biological pattern or characteristic that is used to identify a specific individual.

(2) "Child" means an individual younger than 13 years of age.

(3) "Collect," in the context of data, means to obtain, receive, access, or otherwise acquire the data by any means, including by purchasing or renting the data.

(4) "Data broker" means a business entity whose principal source of revenue is derived from the collecting, processing, or transferring of personal data that the entity did not collect directly from the individual linked or linkable to the data.

(5) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual or to a device linked to that individual.

(6) "Employee" includes an individual who is a director, officer, staff member, trainee, volunteer, or intern of an employer or an individual working as an independent contractor for an employer, regardless of whether the individual is paid, unpaid, or employed on a temporary basis. The term does not include an individual contractor who is a service provider.

(7) "Employee data" means information collected, processed, or transferred by an employer if the information:

(A) is related to:

(i) a job applicant and was collected during the course of the hiring and application process;

(ii) an employee who is acting in a professional capacity for the employer, including the employee's business contact information such as the employee's name, position, title, business telephone number, business address, or business e-mail address;

(iii) an employee's emergency contact information; or

(iv) an employee or the employee's spouse, dependent, covered family member, or beneficiary; and

(B) was collected, processed, or transferred solely for:

(i) a purpose relating to the status of a person described by Paragraph (A)(i) as a current or former job applicant of the employer;

(ii) a purpose relating to the professional activities of an employee described by Paragraph (A)(ii) on behalf of the employer;

(iii) the purpose of having an emergency contact on file for an employee described by Paragraph (A)(iii) and for transferring the information in case of an emergency; and

(iv) the purpose of administering benefits to which an employee described by Paragraph (A)(iv) is entitled or to which another person described by that paragraph is entitled on the basis of the employee's position with the employer.

(8) "Genetic data" means any data, regardless of format, concerning an individual's genetic characteristics. The term includes:

(A) raw sequence data derived from sequencing all or a portion of an individual's extracted DNA; and

(B) genotypic and phenotypic information obtained from analyzing an individual's raw sequence data.

(9) "Individual" means a natural person residing in this state.

(10) "Known child" means a child under circumstances where a data broker has actual knowledge of, or wilfully disregards obtaining actual knowledge of, the child's age.

(11) "Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the information is used by a controller or processor in conjunction with additional information that reasonably links the information to an identified or identifiable individual. The term does not include deidentified data, employee data, or publicly available information.

(12) "Precise geolocation data" means information accessed on a device or technology that shows the past or present physical location of an individual or the individual's device with sufficient precision to identify street-level location information of the individual or device in a range of not more than 1,850 feet. The term does not include location information regarding an individual or device identifiable or derived solely from the visual content of a legally obtained image, including the location of a device that captured the image.

(13) "Process," in the context of data, means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(14) "Publicly available information" means information that:

(A) is lawfully made available through government records;

(B) a business has a reasonable basis to believe is lawfully available to the general public through widely distributed media; or

(C) is lawfully made available by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted access to the information to a specific audience.

(15) "Sensitive data" means:

(A) a government-issued identifier not required by law to be available publicly, including:

(i) a social security number;

(ii) a passport number; or

(iii) a driver's license number;

(B) information that describes or reveals an individual's mental or physical health diagnosis, condition, or treatment;

(C) an individual's financial information, except the last four digits of a debit or credit card number, including:

(i) a financial account number;

(ii) a credit or debit card number; or

(iii) information that describes or reveals the income level or bank account balances of the individual;

(D) biometric data;

(E) genetic data;

(F) precise geolocation data;

(G) an individual's private communication that:

(i) if made using a device, is not made using a device provided by the individual's employer that provides conspicuous notice to the individual that the employer may access communication made using the device; and

(ii) includes, unless the data broker is the sender or an intended recipient of the communication:

(a) the individual's voicemails, e-mails, texts, direct messages, or mail;

(b) information that identifies the parties involved in the communications; and

(c) information that relates to the transmission of the communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call;

(H) a log-in credential, security code, or access code for an account or device;

(I) information identifying the sexual behavior of the individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of the information;

(J) calendar information, address book information, phone or text logs, photos, audio recordings, or videos:

(i) maintained for private use by an individual and stored on the individual's device or in another location; and

(ii) not communicated using a device provided by the individual's employer unless the employee was provided conspicuous notice that the employer may access communication made using the device;

(K) a photograph, film, video recording, or other similar medium that shows the individual or a part of the individual nude or wearing undergarments;

(L) information revealing the video content requested or selected by an individual that is not:

(i) collected by a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming, as that term is defined by 47 U.S.C. Section 613(h)(2); or

(ii) used solely for transfers for independent video measurement;

(M) information regarding a known child;

(N) information revealing an individual's racial or ethnic origin, color, religious beliefs, or union membership;

(O) information identifying an individual's online activities over time accessing multiple Internet websites or online services; or

(P) information collected, processed, or transferred for the purpose of identifying information described by this subdivision.

(16) "Service provider" means a person that receives, collects, processes, or transfers personal data on behalf of, and at the direction of, a business or governmental entity, including a business or governmental entity that is another service provider, in order for the person to perform a service or function with or on behalf of the business or governmental entity.

(17) "Transfer," in the context of data, means to disclose, release, share, disseminate, make available, sell, or license the data by any means or medium.

Sec. 509.002. APPLICABILITY TO CERTAIN DATA. (a) Except as provided by Subsection (b), this chapter applies to personal data from an individual that is collected, transferred, or processed by a data broker.

(b) This chapter does not apply to the following data:

(1) deidentified data, if the data broker:

(A) takes reasonable technical measures to ensure that the data is not able to be used to identify an individual with whom the data is associated;

(B) publicly commits in a clear and conspicuous manner:

(i) to process and transfer the data solely in a deidentified form without any reasonable means for reidentification; and

(ii) to not attempt to identify the information to an individual with whom the data is associated; and

(C) contractually obligates a person that receives the information from the provider:

(i) to comply with this subsection with respect to the information; and

(ii) to require that those contractual obligations be included in any subsequent transfer of the data to another person;

(2) employee data;

(3) publicly available information;

(4) inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive data with respect to an individual; or

(5) data subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.).

Sec. 509.003. APPLICABILITY OF CHAPTER TO CERTAIN ENTITIES. (a) Except as provided by Subsection (b), this chapter applies only to a data broker that, in a 12-month period, derives:

(1) more than 50 percent of the data broker's revenue from processing or transferring personal data that the data broker did not collect directly from the individuals to whom the data pertains; or

(2) revenue from processing or transferring the personal data of more than 50,000 individuals that the data broker did not collect directly from the individuals to whom the data pertains.

(b) This chapter does not apply to:

(1) a service provider, including a service provider that engages in the business of processing employee data for a third-party employer for the sole purpose of providing benefits to the third-party employer's employees;

(2) a person or entity that collects personal data from another person or entity to which the person or entity is related by common ownership or corporate control, provided a reasonable consumer would expect the persons or entities to share data;

(3) a federal, state, tribal, territorial, or local governmental entity, including a body, authority, board, bureau, commission, district, agency, or political subdivision of a governmental entity;

(4) an entity that serves as a congressionally designated nonprofit, national resource center, or clearinghouse to provide assistance to victims, families, child-serving

professionals, and the general public on missing and exploited children issues;

(5) a consumer reporting agency or other person or entity that furnishes information for inclusion in a consumer credit report or obtains a consumer credit report, but only to the extent the person or entity engages in activity regulated or authorized by the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.), including the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living; or

(6) a financial institution subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.).

Sec. 509.004. NOTICE ON WEBSITE OR MOBILE APPLICATION. A data broker that maintains an Internet website or mobile application shall post a conspicuous notice on the website or application that:

(1) states that the entity maintaining the website or application is a data broker;

(2) is clear, not misleading, and readily accessible by the general public, including individuals with a disability; and

(3) contains language provided by rule of the secretary of state for inclusion in the notice.

Sec. 509.005. REGISTRATION. (a) To conduct business in this state, a data broker to which this chapter applies shall register with the secretary of state by filing a registration statement and paying a registration fee of $300.

(b) The registration statement must include:

(1) the legal name of the data broker;

(2) a contact person and the primary physical address, e-mail address, telephone number, and Internet website address for the data broker;

(3) a description of the categories of data the data broker processes and transfers;

(4) a statement of whether or not the data broker implements a purchaser credentialing process;

(5) if the data broker has actual knowledge that the data broker possesses personal data of a known child:

(A) a statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal data of a known child; and

(B) a statement on how the data broker complies with applicable federal and state law regarding the collection, use, or disclosure of personal data from and about a child on the Internet; and

(6) the number of security breaches the data broker has experienced during the year immediately preceding the year in which the registration is filed, and if known, the total number of consumers affected by each breach.

(c) A registration of a data broker may include any additional information or explanation the data broker chooses to provide to the secretary of state concerning the data broker's data collection practices.

(d) A registration certificate expires on the first anniversary of its date of issuance. A data broker may renew a registration certificate by filing a renewal application, in the form prescribed by the secretary of state, and paying a renewal fee in the amount of $300.

Sec. 509.006. REGISTRY OF DATA BROKERS. (a) The secretary of state shall establish and maintain, on its Internet website, a searchable, central registry of data brokers registered under Section 509.005.

(b) The registry must include:

(1) a search feature that allows a person searching the registry to identify a specific data broker; and

(2) for each data broker, the information filed under Section 509.005(b).

Sec. 509.007. PROTECTION OF PERSONAL DATA: COMPREHENSIVE

INFORMATION SECURITY PROGRAM. (a) A data broker conducting business in this state has a duty to protect personal data held by that data broker as provided by this section.

(b) 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 for:

(1) the data broker's size, scope, and type of business;

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

(3) the amount of data stored by the data broker; and

(4) the need for security and confidentiality of personal data stored by the data broker.

(c) The comprehensive information security program required by this section must:

(1) incorporate safeguards that are consistent with the safeguards for protection of personal data and information of a similar character under state or federal laws and regulations applicable to the data broker;

(2) include the designation of one or more employees of the data broker to maintain the program;

(3) require the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other record containing personal data, and the establishment of a process for evaluating and improving, as necessary, the effectiveness of the current safeguards for limiting those risks, including by:

(A) requiring ongoing employee and contractor education and training, including education and training for temporary employees and contractors of the data broker, on the proper use of security procedures and protocols and the importance of personal data security;

(B) mandating employee compliance with policies and procedures established under the program; and

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

(4) include security policies for the data broker's employees relating to the storage, access, and transportation of records containing personal data outside of the broker's physical business premises;

(5) provide disciplinary measures for violations of a policy or procedure established under the program;

(6) include measures for preventing a terminated employee from accessing records containing personal data;

(7) provide policies for the supervision of third-party service providers that include:

(A) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal data consistent with applicable law; and

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

(8) provide reasonable restrictions on physical access to records containing personal data, including by requiring the records containing the data to be stored in a locked facility, storage area, or container;

(9) include regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal data and, as necessary, upgrading information safeguards to limit the risk of unauthorized access to or unauthorized use of personal data;

(10) require the regular review of the scope of the program's security measures that must occur:

(A) at least annually; and

(B) whenever there is a material change in the data broker's business practices that may reasonably affect the security or integrity of records containing personal data;

(11) require the documentation of responsive actions taken in connection with any incident involving a breach of security, including a mandatory post-incident review of each event and the actions taken, if any, to make changes in business practices relating to protection of personal data in response to that event; and

(12) to the extent technically feasible, include the following procedures and protocols with respect to computer system security requirements or procedures and protocols providing a higher degree of security, for the protection of personal data:

(A) the use of secure user authentication protocols that include each of the following features:

(i) controlling user log-in credentials and other identifiers;

(ii) using a reasonably secure method of assigning and selecting passwords or using unique identifier technologies, which may include biometrics or token devices;

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

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

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

(B) the use of secure access control measures that include:

(i) restricting access to records and files containing personal data to only employees or contractors who need access to that personal data to perform the job duties of the employees or contractors; and

(ii) assigning to each employee or contractor with access to a computer containing personal data unique identification and a password, which may not be a vendor-supplied default password, or using another protocol reasonably designed to maintain the integrity of the security of the access controls to personal data;

(C) encryption of:

(i) transmitted records and files containing personal data that will travel across public networks; and

(ii) data containing personal data that is transmitted wirelessly;

(D) reasonable monitoring of systems for unauthorized use of or access to personal data;

(E) encryption of all personal data stored on laptop computers or other portable devices;

(F) for files containing personal data on a system that is connected to the Internet, the use of reasonably current firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal data; and

(G) the use of:

(i) a reasonably current version of system security agent software that must include malware protection and reasonably current patches and virus definitions; or

(ii) a version of system security agent software that is supportable with current patches and virus definitions and is set to receive the most current security updates on a regular basis.

Sec. 509.008. CIVIL PENALTY. (a) A data broker that violates Section 509.004 or 509.005 is liable to this state for a civil penalty as prescribed by this section.

(b) A civil penalty imposed against a data broker under this section:

(1) subject to Subdivision (2), may not be in an amount less than the total of:

(A) $100 for each day the entity is in violation of Section 509.004 or 509.005; and

(B) the amount of unpaid registration fees for each year the entity failed to register in violation of Section 509.005; and

(2) may not exceed $10,000 assessed against the same data broker in a 12-month period.

(c) The attorney general may bring an action to recover a civil penalty imposed under this section. The attorney general may recover reasonable attorney's fees and court costs incurred in bringing the action.

Sec. 509.009. DECEPTIVE TRADE PRACTICE. A violation of Section 509.007 by a data broker constitutes a deceptive trade practice in addition to the practices described by Subchapter E, Chapter 17, and is actionable under that subchapter.

Sec. 509.010. RULES. The secretary of state shall adopt rules as necessary to implement this chapter.

SECTION 2. Not later than December 1, 2023, the secretary of state shall adopt rules necessary to facilitate registration by a data broker under Section 509.005, Business & Commerce Code, as added by this Act, including by incorporating into the rules adequate time for a data broker to comply with Chapter 509, Business & Commerce Code, as added by this Act, following the adoption of the rules.

SECTION 3. Chapter 509, Business & Commerce Code, as added by this Act, applies only to the collection, processing, or transfer of personal data by a data broker on or after December 1, 2023.

SECTION 4. This Act takes effect September 1, 2023.

* * * * *