

By: Johnson, Kolthorst
Menéndez

S.B. No. 2105

A BILL TO BE ENTITLED

AN ACT

1
2 relating to the registration of and certain other requirements
3 relating to data brokers; providing a civil penalty and authorizing
4 a fee.

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

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

8 CHAPTER 509. DATA BROKERS

9 Sec. 509.001. DEFINITIONS. In this chapter:

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

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

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

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

1 data.

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

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

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

13 (A) is related to:

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

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

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

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

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

27 (i) a purpose relating to the status of a

1 person described by Paragraph (A)(i) as a current or former job
2 applicant of the employer;

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

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

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

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

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

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

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

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

25 (11) "Personal data" means any information, including
26 sensitive data, that is linked or reasonably linkable to an
27 identified or identifiable individual. The term includes

1 pseudonymous data when the information is used by a controller or
2 processor in conjunction with additional information that
3 reasonably links the information to an identified or identifiable
4 individual. The term does not include deidentified data, employee
5 data, or publicly available information.

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

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

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

22 (A) is lawfully made available through
23 government records;

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

27 (C) is lawfully made available by a consumer, or

1 by a person to whom a consumer has disclosed the information, unless
2 the consumer has restricted access to the information to a specific
3 audience.

4 (15) "Sensitive data" means:

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

7 (i) a social security number;

8 (ii) a passport number; or

9 (iii) a driver's license number;

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

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

16 (i) a financial account number;

17 (ii) a credit or debit card number; or

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

20 (D) biometric data;

21 (E) genetic data;

22 (F) precise geolocation data;

23 (G) an individual's private communication that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 (M) information regarding a known child;

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

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

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

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

27 (17) "Transfer," in the context of data, means to

1 disclose, release, share, disseminate, make available, sell, or
2 license the data by any means or medium.

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

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

8 (1) deidentified data, if the data broker:

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

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

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

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

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

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

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

26 (2) employee data;

27 (3) publicly available information;

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

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

6 Sec. 509.003. APPLICABILITY OF CHAPTER TO CERTAIN ENTITIES.

7 (a) Except as provided by Subsection (b), this chapter applies only
8 to a data broker that, in a 12-month period, derives:

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

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

17 (b) This chapter does not apply to:

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

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

27 (3) a federal, state, tribal, territorial, or local

1 governmental entity, including a body, authority, board, bureau,
2 commission, district, agency, or political subdivision of a
3 governmental entity;

4 (4) an entity that serves as a congressionally
5 designated nonprofit, national resource center, or clearinghouse
6 to provide assistance to victims, families, child-serving
7 professionals, and the general public on missing and exploited
8 children issues;

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

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

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

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

27 (2) is clear, not misleading, and readily accessible

1 by the general public, including individuals with a disability; and

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

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

8 (b) The registration statement must include:

9 (1) the legal name of the data broker;

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

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

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

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

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

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

26 (6) the number of security breaches the data broker
27 has experienced during the year immediately preceding the year in

1 which the registration is filed, and if known, the total number of
2 consumers affected by each breach.

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

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

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

16 (b) The registry must include:

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

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

21 Sec. 509.007. PROTECTION OF PERSONAL DATA: COMPREHENSIVE
22 INFORMATION SECURITY PROGRAM. (a) A data broker conducting
23 business in this state has a duty to protect personal data held by
24 that data broker as provided by this section.

25 (b) A data broker shall develop, implement, and maintain a
26 comprehensive information security program that is written in one
27 or more readily accessible parts and contains administrative,

1 technical, and physical safeguards that are appropriate for:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26 (9) include regular monitoring to ensure that the
27 program is operating in a manner reasonably calculated to prevent

1 unauthorized access to or unauthorized use of personal data and, as
2 necessary, upgrading information safeguards to limit the risk of
3 unauthorized access to or unauthorized use of personal data;

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

6 (A) at least annually; and

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

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

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

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

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

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

27 (iii) controlling data security passwords

1 to ensure that the passwords are kept in a location and format that
2 do not compromise the security of the data the passwords protect;

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

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

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

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

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

20 (C) encryption of:

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

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

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

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

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

8 (G) the use of:

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

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

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

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

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

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

25 (B) the amount of unpaid registration fees for
26 each year the entity failed to register in violation of Section
27 509.005; and

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

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

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

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

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

20 SECTION 3. Chapter 509, Business & Commerce Code, as added
21 by this Act, applies only to the collection, processing, or
22 transfer of personal data by a data broker on or after December 1,
23 2023.

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