2022 Regular Session

HOUSE BILL NO. 987

BY REPRESENTATIVE DESHOTEL

PRIVACY: Provides relative to the protection of data

AN ACT

To amend and reenact R.S. 44:4.1(B)(35) and to enact Chapter 12-B of Title 51 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 51:1381 through 1397, relative to data privacy; to provide definitions; to provide for applicability; to provide for consumer rights; to require a response to a request; to provide for the responsibilities of a processor and a controller; to provide for deidentified data; to provide limitations; to provide for investigative powers; to provide for enforcement; to provide for a civil fine; to provide for a data assessment; to provide for a public records exception; to create an account; to require a report; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. R.S. 44:4.1(B)(35) is hereby amended and reenacted to read as follows:

§4.1. Exceptions

* * *

B. The legislature further recognizes that there exist exceptions, exemptions, and limitations to the laws pertaining to public records throughout the revised statutes and codes of this state. Therefore, the following exceptions, exemptions, and limitations are hereby continued in effect by incorporation into this Chapter by citation:

* * *

(35) R.S. 51:710.2(B), 705, 706, 936, 1395, 1404, 1926, 1934, 2113, 2182, 2262, 2318, 2389

* * *

Section 2. Chapter 12-B of Title 51 of the Louisiana Revised Statutes of 1950, comprised of R.S. 51:1381 through 1397, is hereby enacted to read as follows:

CHAPTER 12-B. LOUISIANA CONSUMER PRIVACY ACT

§1381. Short title

This Chapter shall be known and may be cited as the "Louisiana Consumer Privacy Act".

§1382. Definitions

As used in this Chapter, the following words have the following meanings:

(1) "Account" means the consumer privacy restricted account established in R.S. 51:1396.

(2) "Affiliate" means an entity that satisfies either of the following criteria:

(a) Controls, is controlled by, or is under common control with another entity.

(b) Shares common branding with another entity.

(3) "Aggregated data" means information that relates to a group or category of consumers that satisfies all of the following criteria:

(a) All individual consumer identities have been removed from the information.

(b) The information is not linked or reasonably linkable to any consumer.

(4) "Air carrier" means the same as that term is defined in 49 U.S.C. 40102.

(5) "Authenticate" means to use reasonable means to determine that a consumer's request to exercise the rights described in R.S. 51:1385 is made by the consumer who is entitled to exercise those rights.

(6)(a) "Biometric data" means data generated by automatic measurements of an individual's unique physical, physiological, or biological characteristics that allow or confirm the unique identity of a specific individual.

(b) "Biometric data" includes data described in Subparagraph (a) of this Paragraph that is generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual.

(c) "Biometric data" does not include any of the following:

(i) A physical or digital photograph.

(ii) A video or audio recording.

(iii) Information captured from a patient in a healthcare setting.

(iv) Information collected, used, or stored for treatment, payment, or healthcare operations as those terms are defined in 45 CFR Parts 160, 162, and 164.

(7) "Business associate" means the same as that term is defined in 45 CFR 160.103.

(8) "Child" means an individual younger than thirteen years old.

(9)(a) "Consent" means a clear and affirmative act by a consumer that unambiguously indicates the consumer's voluntary, specific, and informed agreement to allow a person to process personal data related to the consumer.

(b) "Consent" does not include the following:

(i) Acceptance of general or broad terms of use or a similar document that contains descriptions of personal data processing along with other unrelated information.

(ii) Hovering over, muting, pausing, or closing a given piece of content.

(10)(a) "Consumer" means an individual who is a resident of this state acting in an individual or household context.

(b) "Consumer" does not include an individual acting in an employment or commercial context.

(11) "Control" or "controlled" as used in Paragraph (2) of this Section means any of the following:

(a) Ownership of or the power to vote more than fifty percent of the outstanding shares of any class of voting securities of an entity.

(b) Control in any manner over the election of a majority of the directors or of the individuals exercising similar functions.

(c) The power to exercise controlling influence of the management of an entity.

(12) "Controller" means a person doing business in this state who determines the purposes for and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others.

(13) "Covered entity" means the same as that term is defined in 45 CFR 160.103.

(14) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified individual, device, or household.

(15) "Director" means the director of the consumer protection section of the Department of Justice.

(16) "Division" means the consumer protection section of the Department of Justice.

(17) "Governmental entity" means any board, authority, commission, department, office, division, or agency of this state or any of its political subdivisions.

(18) "Healthcare facility" means an institution providing medical services or a healthcare setting, including but not limited to a hospital or other licensed inpatient center, an ambulatory surgical or treatment center, a skilled nursing center, a residential treatment center, a rehabilitation center, and a diagnostic, laboratory, or imaging center.

(19) "Healthcare provider" means any person licensed, certified, or registered in this state to provide healthcare services, including but not limited to physicians, hospitals, home health agencies, chiropractors, pharmacies, and dentists.

(20) "Identified individual" or "identifiable individual" means an individual who can be readily identified, either directly or indirectly, in particular or by

reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(21) "Institution of higher education" means a public or private institution of higher education.

(22) "Political subdivision" means a parish, municipality, and any other unit of local government, including but not limited to a school board or a special district, authorized by law to perform governmental functions.

(23) "Nonprofit corporation" means any of the following:

(a) A corporation incorporated in accordance with the laws of this state and subject to the provisions of the Nonprofit Corporation Law, R.S. 12:01 et seq.

(b) A corporation incorporated in accordance with the laws of another state that would be considered a nonprofit corporation if it were incorporated in accordance with the laws of this state.

(24)(a) "Personal data" means information that is linked or reasonably linkable to an identified individual or an identifiable individual.

(b) "Personal data" does not include deidentified data.

(25) "Process" means an operation or set of operations performed on personal data, including but not limited to collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(26) "Processor" means a person who processes personal data on behalf of a controller.

(27) "Protected health information" means the same as that term is defined in 45 CFR 160.103.

(28) "Publicly available information" means information that satisfies any of the following criteria:

(a) It is lawfully obtainable by a person from a record of a governmental entity.

(b) It is obtainable by a person who reasonably believes a consumer or a widely- distributed media source has lawfully made available to the general public.

(c) It is obtainable from a person to whom the consumer disclosed the information, if the consumer has not restricted the information to a specific audience.

(29) "Right" means a consumer right described in R.S. 51:1385.

(30)(a) "Sale", "sell", or "sold" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party.

(b) "Sale", "sell", or "sold" does not include:

(i) A controller's disclosure of personal data to a processor who processes the personal data on behalf of the controller.

(ii) A controller's disclosure of personal data to an affiliate of the controller.

(iii) Considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations.

(iv) The disclosure or transfer of personal data if a consumer directs a controller to do either of the following:

(aa) Disclose the personal data.

(bb) Interact with one or more third parties.

(v) A consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a child.

(vi) The disclosure of information, if the consumer satisfies all of the following criteria:

(aa) Intentionally makes available to the general public via a channel of mass media.

(bb) Does not restrict the information to a specific audience.

(vii) A controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, an acquisition, or a bankruptcy in which the third party assumes control of all or part of the controller's assets.

(31)(a) "Sensitive data" means any of the following:

(i) Personal data that reveals any of the following:

(aa) An individual's racial or ethnic origin.

(bb) An individual's religious beliefs.

(cc) An individual's sexual orientation.

(dd) An individual's citizenship or immigration status.

(ee) Information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional.

(ii) The processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual.

(iii) Specific geolocation data.

(iv) Biometric data.

(b) "Sensitive data" does not include personal data that reveals any of the following, if processed in the manner provided:

(i) Racial or ethnic origin, if the personal data is processed by a video communication service.

(ii) Any information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional, if the personal data is processed by a person licensed to provide health care in accordance with the laws of this state.

(32)(a) "Specific geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of one thousand eight hundred fifty feet or fewer.

(b) "Specific geolocation data" does not include either of the following:

(i) The content of a communication.

(ii) Any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(33)(a) "Targeted advertising" means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(b) "Targeted advertising" does not include any of the following:

(i) Advertising based on a consumer's activities within a controller's website or online application or any affiliated website or online application.

(ii) Advertising based on the context of a consumer's current search query or visit to a website or online application.

(iii) Advertising directed to a consumer in response to the consumer's request for information, products, services, or feedback.

(iv) Processing personal data solely to measure or report on advertising performance, advertising reach, or advertising frequency.

(34) "Third party" means a person other than the following:

(a) The consumer, controller, or processor.

(b) An affiliate or contractor of the controller or the processor.

(35) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process that satisfies all of the following criteria:

(a) Derives independent economic value, actual or potential, from not being generally known or readily ascertainable by proper means by other persons who can obtain economic value from the information's disclosure or use.

(b) Is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

§1383. Applicability

A. The provisions of this Chapter apply to any controller or processor who conducts business in this state or produces a product or service that is targeted to consumers who are residents of this state if the controller or processor satisfies both of the following:

(1) Has annual revenue of twenty-five million dollars or more.

(2) Satisfies any of the following criteria:

(a) During a calendar year, controls or processes the personal data of at least one hundred thousand consumers.

(b) Derives over fifty percent of the entity's gross revenue from the sale of personal data and controls or processes the personal data of twenty-five thousand or more consumers.

B. The provisions of this Chapter do not apply to any of the following:

(1) A governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity.

(2) A tribe.

(3) An institution of higher education.

(4) A nonprofit corporation.

(5) A covered entity.

(6) A business associate.

(7) Protected health information for purposes of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq., and related regulations.

(8) Patient identifying information for purposes of 42 CFR Part 2.

(9) Identifiable private information for purposes of the Federal Policy for the Protection of Human Subjects, 45 CFR Part 46.

(10) Identifiable private information or personal data collected as part of human subjects research pursuant to or under the same standards as either of the following:

(a) The good clinical practice guidelines issued by the International Council for Harmonisation.

(b) The Protection of Human Subjects as provided in 21 CFR Part 50 and Institutional Review Boards as provided in 21 CFR Part 56.

(11) Personal data used or shared in research conducted in accordance with one or more of the requirements described in Paragraph (9) of this Subsection.

(12) Information and documents created specifically for, and collected and maintained by the Louisiana Department of Health.

(13) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq., and related regulations.

(14) Patient safety work product for purposes of 42 CFR Part 3.

(15) Information that satisfies all of the following criteria:

(a) Deidentified in accordance with the requirements for deidentification set forth in 45 CFR Part 164.

(b) Derived from any of the healthcare-related information listed in Paragraphs (7) through (14) of this Subsection.

(16) Information originating from or indistinguishably intermingled with information provided for in Paragraphs (7) through (14) of this Subsection that is maintained by either of the following:

(a) A healthcare facility or healthcare provider.

(b) A program or a qualified service organization as defined in 42 CFR 2.11.

(17) Information used only for public health activities and purposes as described in 45 CFR 164.512.

(18)(a) An activity by any of the following, if all of the criteria provided in Subparagraphs (b) and (c) of this Paragraph are satisfied:

(i) A consumer reporting agency, as defined in 15 U.S.C. Sec. 1681a.

(ii) A furnisher of information, as set forth in 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in 15 U.S.C. Sec. 1681a.

(iii) A user of a consumer report, as set forth in 15 U.S.C. Sec. 1681b.

(b) The activity is subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

(c) The activity involves the collection, maintenance, disclosure, sale, communication, or use of any personal data that bears on any of the following relative to the consumer:

(i) Credit worthiness.

(ii) Credit standing.

(iii) Credit capacity.

(iv) Character.

(v) General reputation.

(vi) Personal characteristics.

(vii) Mode of living.

(19) A financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq. and related regulations.

(20) Personal data collected, processed, sold, or disclosed in accordance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.

(21) Personal data regulated by the Family Education Rights and Privacy Act, 20 U.S.C. 1232g and related regulations.

(22) Personal data collected, processed, sold, or disclosed in accordance with the Farm Credit Act of 1971, 12 U.S.C. 2001 et seq.

(23) Data that is processed or maintained in any of the following manners:

(a) In the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent the collection and use of the data are related to the individual's role.

(b) As the emergency contact information of an individual described in Subparagraph (a) of this Paragraph and used for emergency contact purposes.

(c) To administer benefits for another individual relating to an individual described in Subparagraph (a) of this Paragraph and used for the purpose of administering the benefits.

(24) An individual's processing of personal data for purely personal or household purposes.

(25) An air carrier.

C. A controller is in compliance with any obligation to obtain parental consent pursuant to this Chapter if the controller complies with the verifiable parental consent mechanisms as provided in the Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq. and the act's implementing regulations and exemptions.

D. This Chapter does not require a person to take any action in conflict with the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq. or related regulations.

§1384. Preemption

A. The provisions of this Chapter supersede and preempt any ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or processor.

B. Any reference to federal law in this Chapter includes any rules or regulations promulgated pursuant to that federal law.

§1385. Consumer rights

A. A consumer has the right to do all of the following:

(1) Confirm whether a controller is processing the consumer's personal data.

(2) Access the consumer's personal data.

(3) Obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that satisfies all of the following:

(a) To the extent technically feasible, is portable.

(b) To the extent practicable, is readily usable.

(c) Allows the consumer to transmit the data to another controller without impediment, if the processing is carried out by automated means.

(4) Correct inaccuracies in the consumer's personal data.

(5) Delete the consumer's personal data.

(6) A consumer has the right to opt out of the processing of the consumer's personal data for either of the following purposes:

(a) Targeted advertising.

(b) The sale of personal data.

B. Nothing in this Section requires a person to cause a breach of a security system as defined in R.S. 51:3073.

§1386. Exercising consumer rights

A. A consumer may exercise a right provided for in R.S. 51:1385 by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise.

B. In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise a right on the child's behalf.

C. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer shall exercise a right on the consumer's behalf.

§1387. Controller's response to request

A. Subject to the other provisions of this Chapter, a controller shall comply with a consumer's request to exercise a right pursuant to R.S. 51:1386.

B.(1) Within forty-five days of receiving a request to exercise a right, the controller shall do both of the following:

(a) Take action on the consumer's request.

(b) Inform the consumer of any action taken on the consumer's request.

(2) The controller may extend the initial forty-five-day period by an additional forty-five days, if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller. The controller may extend the period only once.

(3) If a controller extends the initial forty-five-day period, before the initial forty-five-day period expires, the controller shall do all of the following:

(a) Inform the consumer of the extension, including the length of the extension.

(b) Provide the reasons the extension is reasonably necessary as described in Paragraph (2) of this Subsection.

(4) The forty-five-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent, and the controller is not able to authenticate the request before the forty-five-day period expires.

(5) If, in accordance with the provision of this Section, a controller chooses not to take action on a consumer's request, the controller shall, within forty-five days after the day on which the controller receives the request, inform the consumer of the reasons for not taking action.

D.(1) A controller may not charge a fee for information in response to a request, unless the request is the consumer's second or subsequent request during the same twelve-month period.

(2)(a) Notwithstanding Paragraph (1) of this Subsection, a controller may charge a reasonable fee to cover the administrative costs of complying with a request or may refuse to act on a request, if any of the following is true:

(i) The request is excessive, repetitive, technically infeasible, or manifestly unfounded.

(ii) The controller reasonably believes the consumer's primary purpose in submitting the request was something other than exercising a right.

(iii) The request, individually or as part of an organized effort, harasses, disrupts, or imposes an undue burden on the resources of the controller's business.

(b) A controller who charges a fee or refuses to act in accordance with this Subsection bears the burden of demonstrating the request satisfied one or more of the criteria described in Subparagraph (a) of this Paragraph.

E. If a controller is unable to authenticate a consumer request to exercise a right described in R.S. 51:1385 using commercially-reasonable efforts, the controller is not required to comply with the request and may request that the consumer provide additional information reasonably necessary to authenticate the request.

§1388. Responsibility according to role

A. A processor shall do both of the following:

(1) Adhere to the controller's instructions.

CODING: Words in ~~struck through~~ type are deletions from existing law; words underscored are additions.

(2) Taking into account the nature of the processing and information available to the processor, by appropriate technical and organizational measures, insofar as reasonably practicable, assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of a security system described in R.S. 51:3073.

B. Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that satisfies all of the following criteria:

(1) Clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations.

(2) Requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data.

(3) Requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

C.(1) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed.

(2) A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.

§1389. Responsibilities of controllers

A.(1) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes all of the following:

(a) The categories of personal data processed by the controller.

(b) The purposes for which the categories of personal data are processed.

(c) How consumers may exercise a right.

(d) The categories of personal data that the controller shares with third parties, if any.

(e) The categories of third parties, if any, with whom the controller shares personal data.

(2) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of each of the following:

(a) Processing for targeted advertising.

(b) Sale of the consumer's personal data.

B.(1) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to achieve all of the following:

(a) Protect the confidentiality and integrity of personal data.

(b) Reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.

(2) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

C. Except as otherwise provided for in this Chapter, a controller shall not process sensitive data collected from a consumer without doing either of the following:

(1) Presenting the consumer with clear notice and an opportunity to opt out of the processing, prior to the data being processed.

(2) Processing the data in accordance with the Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq., and the act's implementing regulations and exemptions, in the case of the processing of personal data concerning a known child.

D.(1) A controller may not discriminate against a consumer for exercising a right by doing any of the following:

(a) Denying a good or service to the consumer.

(b) Charging the consumer a different price or rate for a good or service.

(c) Providing the consumer a different level of quality of a good or service.

(2) This Subsection does not prohibit a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee or at a discount, if either of the following is true:

(a) The consumer has opted out of targeted advertising.

(b) The offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

E. Notwithstanding the provisions of Subsection D of this Section, a controller is not required to provide a product, service, or functionality to a consumer if all of the following are satisfied:

(1) The consumer's personal data is or the processing of the consumer's personal data is reasonably necessary for the controller to provide the consumer the product, service, or functionality.

(2) The consumer does not do either of the following:

(a) Provide the consumer's personal data to the controller.

(b) Allow the controller to process the consumer's personal data.

F. Any provision of a contract that purports to waive or limit a consumer's right in accordance with this Chapter is absolutely null.

§1390. Processing deidentified data

A. A controller of deidentified data shall:

(1) Take reasonable measures to ensure that a person cannot associate the data with an individual.

(2) Publicly commit to maintain and use the data only in its deidentified form and to not attempting to reidentify the data.

(3) Contractually obligate any recipient of the data to comply with the requirements of this Subsection.

B. The provisions of this Chapter do not require a controller or processor to do any of the following:

(1) Reidentify deidentified data.

(2) Maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data.

(3)(a) Comply with an authenticated consumer request to exercise a right as described in R.S. 51:1386, if the controller complies with Subparagraph (b) of this Paragraph and either of the following is satisfied:

(i) The controller is not reasonably capable of associating the request with the personal data.

(ii) It would be unreasonably burdensome for the controller to associate the request with the personal data.

(b) For purposes of Subparagraph (a) of this Paragraph, the controller does not do any of the following:

(i) Use the personal data to recognize or respond to the consumer who is the subject of the personal data.

(ii) Associate the personal data with other personal data about the consumer.

(iii) Sell or otherwise disclose the personal data to any third party other than a processor, except as otherwise permitted in this Chapter.

C. A controller who uses deidentified data shall take reasonable steps to ensure the processor does all of the following:

(1) Complies with any contractual obligation to which the deidentified data is subject.

(2) Promptly addresses any breach of a contractual obligation described in Paragraph (1) of this Subsection.

§1391. Limitations

A. The requirements described in this Chapter do not restrict a controller's or processor's ability to do any of the following:

(1) Comply with a federal, state, or local law, rule, or regulation.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity.

(3) Cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend a legal claim.

(5) Provide a product or service requested by a consumer or a parent or legal guardian of a child.

(6) Perform a contract to which the consumer or the parent or legal guardian of a child is a party, including fulfilling the terms of a written warranty or taking steps at the request of the consumer or parent or legal guardian prior to entering into the contract with the consumer.

(7) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual.

(8)(a) Detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity.

(b) Investigate, report, or prosecute a person responsible for an action described in Subparagraph (a) of this Paragraph.

(9)(a) Preserve the integrity or security of systems.

(b) Investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable.

(10) If the controller discloses the processing in a notice described in R.S. 51:1389, engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws.

(11) Assist another person with an obligation described in this Section.

(12) Process personal data to do any of the following:

(a) Conduct internal analytics or other research to develop, improve, or repair a controller's or processor's product, service, or technology

(b) Identify and repair technical errors that impair existing or intended functionality.

(c) Effectuate a product recall.

(13) Process personal data to perform an internal operation that is either of the following:

(a) Reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller.

(b) Otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or a parent or legal guardian of a child or the performance of a contract to which the consumer or a parent or legal guardian of a child is a party.

(14) Retain a consumer's email address to comply with the consumer's request to exercise a right.

B. This Chapter does not apply if a controller's or processor's compliance with this Chapter does any of the following:

(1) Violates an evidentiary privilege provided in the laws of this state.

(2) As part of a privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege provided in the laws of this state.

(3) Adversely affects the privacy or other rights of any person.

C. A controller or processor is not in violation of this Chapter if all of the following are true:

(1) The controller or processor discloses personal data to a third-party controller or processor in compliance with this Chapter.

(2) The third party processes the personal data in violation of this Chapter.

(3) The disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of this Chapter.

D. If a controller processes personal data in accordance with an exemption described in Subsection C of this Section, the controller bears the burden of demonstrating that the processing qualifies for the exemption.

E. Nothing in this Chapter requires a controller, processor, third party, or consumer to disclose a trade secret.

§1392. No private cause of action

A violation of this Chapter does not provide a basis for, nor is a violation of this Chapter subject to, a private right of action pursuant to this Chapter or any other law.

§1393. Investigative powers

A. The division shall establish and administer a system to receive consumer complaints regarding a controller's or processor's alleged violation of this Chapter.

B.(1) The division may investigate a consumer complaint to determine whether the controller or processor violated or is violating this Chapter.

(2) If the director has reasonable cause to believe that substantial evidence exists that a person identified in a consumer complaint is in violation of this Chapter, the director shall refer the matter to the attorney general.

(3) Upon request, the division shall provide consultation and assistance to the attorney general in enforcing this Chapter.

§1394. Enforcement powers of the attorney general

A. The attorney general has the exclusive authority to enforce this Chapter.

B. Upon referral from the division, the attorney general may initiate an enforcement action against a controller or processor for a violation of this Chapter.

C.(1) At least thirty days before the day on which the attorney general initiates an enforcement action against a controller or processor, the attorney general shall provide the controller or processor with all of the following:

(a) Written notice identifying each provision of this Chapter the attorney general alleges the controller or processor has violated or is violating.

(b) An explanation of the basis for each allegation.

(2) The attorney general may not initiate an action if the controller or processor does all of the following:

(a) Cures the noticed violation within thirty days after the day on which the controller or processor receives the written notice described in Paragraph (1) of this Subsection.

(b) Provides the attorney general an express written statement that attests to both of the following:

(i) The violation has been cured.

(ii) No further violation of the cured violation will occur.

(3) The attorney general may initiate an action against a controller or processor who does either of the following:

(a) Fails to cure a violation after receiving the notice described in Paragraph (1) of this Subsection.

(b) After curing a noticed violation and providing a written statement in accordance with Paragraph (2) of this Subsection, continues to violate this Chapter.

(4) In an action described in this Section, the attorney general may recover all of the following:

(a) Actual damages to the consumer.

(b) For each violation described in Paragraph (3) of this Subsection, a civil fine in an amount not to exceed seven thousand five hundred dollars.

D. All money received from an action pursuant to this Chapter shall be deposited into the Consumer Privacy Account established in R.S. 51:1396.

E. If more than one controller or processor are involved in the same processing in violation of this Chapter, the liability for the violation shall be allocated among the controllers or processors according to the principles of comparative fault.

§1395. Data protection assessments

A. A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired on or after the effective date of this Chapter that present a heightened risk of harm to a consumer.

B. For purposes of this Section, "processing that presents a heightened risk of harm to a consumer" includes all of the following:

(1) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of any of the following:

(a) Unfair or deceptive treatment of consumers.

(b) Unlawful disparate impact on consumers.

(c) Financial or physical injury to consumers.

(d) An intrusion, physical or otherwise, upon the solitude or seclusion, or the private affairs or concerns of consumers, if the intrusion would be offensive to a reasonable person.

(e) Other substantial injury to consumers.

(2) Selling personal data.

(3) Processing sensitive data.

C. Data protection assessments shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

D. A controller shall make the data protection assessment available to the attorney general upon request. The attorney general may evaluate the data protection assessment for compliance with the duties provided for in this Chapter. Data protection assessments are confidential and exempt from public inspection and copying in accordance with the Public Records Law as provided in R.S. 44:1 et seq. The disclosure of a data protection assessment pursuant to a request from the attorney general pursuant to this Subsection does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.

E. A single data protection assessment may address a comparable set of processing operations that include similar activities.

F. Data protection assessment requirements apply to processing activities created or generated after December 1, 2023.

§1396. Consumer privacy restricted account

A. There is created a restricted account known as the "Consumer Privacy Account".

B. The account shall be funded by money received through civil enforcement actions pursuant to this Chapter.

C. Upon appropriation, the division or the attorney general may use money deposited into the account for any of the following:

(1) Investigative and administrative costs incurred by the division in investigating consumer complaints alleging violations of this Chapter.

(2) Recovery of costs and attorney fees accrued by the attorney general in enforcing this Chapter.

(3) Providing consumer and business education regarding any of the following:

(a) Consumer rights pursuant to this Chapter.

(b) Compliance with the provisions of this Chapter for controllers and processors.

D. If the balance in the account exceeds four million dollars at the close of any fiscal year, the state treasurer shall transfer the amount that exceeds four million dollars into the state general fund.

§1397. Attorney general report

A. The attorney general and the division shall compile a report composed of all of the following:

(1) An evaluation of the liability and enforcement provisions of this Chapter, including the effectiveness of the attorney general's and the division's efforts to enforce this Chapter.

(2) A summary of the data protected and not protected by this Chapter including, with reasonable detail, a list of the types of information that are publicly available from local, state, and federal government sources.

B. The attorney general and the division may update the report as new information becomes available.

C. The attorney general and the division shall submit the report to the House Committee on Commerce and Senate Committee on Commerce, Consumer Protection, and International Affairs before July 1, 2025.

Section 3. This Act shall become effective on December 31, 2023.

DIGEST

The digest printed below was prepared by House Legislative Services. It constitutes no part of the legislative instrument. The keyword, one-liner, abstract, and digest do not constitute part of the law or proof or indicia of legislative intent. [R.S. 1:13(B) and 24:177(E)]

HB 987 Reengrossed 2022 Regular Session Deshotel

Abstract: Establishes consumer rights relative to personal data processing.

Applicability

Proposed law provides that a controller is a person doing business in this state who determines the purposes for and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others.

Proposed law provides that a processor is a person who processes personal data on behalf of a controller.

Proposed law applies to a controller or a processor who conducts business in this state or targets a product or service to residents of this state, has annual revenue of at least $25,000,000, and satisfies either of the following:

(1) During a calendar year, controls or processes the personal data of at least 100,000 consumers.

(2) Derives over 50% of his gross revenue from selling personal data and controls or processes the personal data of at least 25,000 consumers.

Proposed law does not apply to any of the following:

(1) A governmental agency or a third party who has a contract with that governmental entity and acting on the entity's behalf.

(2) A tribe.

(3) An institution of higher education.

(4) A nonprofit corporation.

(5) A covered entity.

(6) A business associate.

(7) Certain protected health information.

(8) Certain identifying information.

(9) Certain information collected, processed, sold, or regulated pursuant to federal law.

(10) Information that has become intermingled with and indistinguishable from certain exempted information.

(11) Activity by a consumer reporting agency, a furnisher of information, or a user of a consumer report, if the activity is subject to the federal fair credit reporting act and involves the collection, maintenance, disclosure, sale, communication, or use of any personal data that bears on certain enumerated factors.

(12) A financial institution governed by federal law.

(13) Data that is processed or maintained relative to employment, emergency contact information, or administration of benefits.

(14) Personal or household processing.

(15) An air carrier.

Consumer Rights

Proposed law provides that a consumer is an individual who is a resident of this state acting in an individual or household context

Proposed law provides that a consumer has the right to do all of the following:

(1) Confirm whether a controller is processing his data.

(2) Access his personal data.

(3) Obtain a copy of his personal data.

(4) Correct inaccuracies in the personal data.

(5) Delete the personal data.

(6) Opt out of the processing of data for the purposes of targeted advertising or the sale of personal data.

A consumer or legal representative of the consumer may exercise the rights provided in proposed law by submitting a request to the controller, in a means prescribed by the controller.

Proposed law requires a controller to comply with a consumers request to exercise a right provided for in proposed law and further requires the controller take action and notify the consumer of such action within 45 days of receipt of the request. Proposed law allows the controller to extend the response time by an additional 45 days if reasonably necessary. The controller is required to notify the consumer if the time period for action is extended and provide a reason for the extension. Proposed law does not require a controller to comply with the 45-day limit if he reasonably suspects fraud and cannot authenticate the request prior to lapse of the 45 days. If a controller chooses not to take action on a request, proposed law requires the controller to notify the consumer of the reason for not taking action within 45 days of receiving the request.

Proposed law prohibits the controller from charging a fee for information in response to a request, unless any of the following is true:

(1) The request is the consumer's second or subsequent request during the same 12-month period.

(2) The request is excessive, repetitive, technically infeasible, or manifestly unfounded.

(3) The controller believes that the consumer's primary purpose in making the request was not to exercise a right provided in proposed law.

(4) The request harasses, disrupts, or places an undue burden on the controller's business.

A controller who charges a fee based on the exceptions in proposed law bears the burden of proving that the necessary criteria is met. Proposed law allows a controller to request additional information from a consumer if reasonably necessary to respond to the request.

Responsibilities of Processors and Controllers

Proposed law requires a processor to adhere to the controller's instructions and assist the controller in meeting his obligations, to the extent practicable.

Prior to processing data on behalf of a controller, proposed law requires the processor and controller to enter into a contract. Proposed law requires that the contract contain clear instructions, a duty of confidentiality, and certain provisions relative to subcontractors.

Proposed law requires a controller to provide consumers with a clear and accessible privacy notice containing all of the following:

(1) The categories of data processed by the controller.

(2) The purposes for which the data is being processed.

(3) How consumers can exercise a right provided in proposed law.

(4) The categories of data the controller shares with third party.

(5) The categories of third parties the controller shares data with.

Proposed law requires a controller to disclose to the consumer the manner in which he may opt out of processing for targeted advertising or sale of his data.

Proposed law requires a controller to create and maintain reasonable and appropriate data security practices that protect the confidentiality and integrity of personal data and reduce harm to consumers.

Proposed law prohibits a controller from processing sensitive data without first notifying the consumer of his right to opt out. Proposed law defers to federal law if the personal data belongs to a child.

Proposed law prohibits a controller from discriminating against a consumer for exercising a right provided in proposed law. However, does not require a controller to provide a product, service, or functionality to a consumer in certain circumstances.

Proposed law requires a controller of deidentified data to take reasonable measures to ensure that a person cannot associate the data with an individual, publicly commit to maintain and use the data only in its deidentified form, and contractually obligate any data recipient to comply with proposed law.

Proposed law does not require a controller or processor to do any of the following, as long as the controller does not engage in certain prohibited activity:

(1) Reidentify certain data.

(2) Maintain data in an identifiable form.

(3) Comply with a request that is not reasonably associated with the personal data or it would be unreasonably burdensome to do so.

Proposed law requires a controller who uses deidentified data to take reasonable steps to ensure that the processor complies with all contractual obligations relative to that data and to promptly address any breach of the contract.

Limitations of Proposed Law

Proposed law provides that proposed law does not restrict a controller or processor from doing any of the following:

(1) Complying with any law or legal order.

(2) Cooperating with law enforcement.

(3) Participating in a legal claim.

(4) Providing a requested service or product.

(5) Performing a contract.

(6) Protecting an interest essential for life or physical safety.

(7) Taking necessary steps in response to certain incidents.

(8) Taking actions relative to the integrity or security of systems.

(9) Engaging in certain research.

(10) Assisting another person in exercising a right provided in proposed law.

(11) Processing personal data for certain purposes.

(12) Retaining a consumer's email address to comply with his request.

Proposed law does not apply if compliance by the controller or processor would result in a violation of an evidentiary rule or privilege or would adversely affect the privacy rights of any person.

Data Protection Assessment

Proposed law requires a controller to conduct and document a data protection assessment prior to engaging in processing that presents a heightened risk of harm to a consumer.

Proposed law provides a list of processing activities that are considered to present a heightened risk of harm to a consumer.

Proposed law provides that data protection assessments are confidential and exempt from the Public Records Law.

Investigations and Enforcement

Proposed law requires the consumer protection section of the Dept. of Justice (section) establish and administer a system to receive consumer complaints.

Proposed law allows the section to investigate complaints and refer the matter to the attorney general if a violation is substantiated.

The attorney general has the exclusive authority to enforce proposed law.

Proposed law requires the attorney general to provide notice and explanation to a controller or processor at least 30 days prior to initiating an enforcement action.

If the controller or processor cures the noticed violation within 30 days of receipt of notice and provides attestation to the attorney general, proposed law prohibits the attorney general from initiating the action.

The attorney general may recover actual damages to the consumer and up to $7,500 per violation of proposed law.

Proposed law creates the Consumer Privacy Account (account) where all monies received from an action arising out of proposed law are to be deposited.

The money in the account may be used for investigative and administrative costs, recovery of costs and attorney's fees, and consumer and business education programs.

If the balance in the account exceeds $4,000,000 at the close of any fiscal year, all funds in excess of $4,000,000 are to be deposited into the general fund.

Proposed law requires the section and the attorney general to submit a report evaluating and summarizing various aspects of proposed law. The report is to be submitted to the House and Senate commerce committees before July 1, 2025.

Miscellaneous Provisions

Proposed law cites federal law as the operating standard for compliance with any obligation to obtain parental consent.

Proposed law preempts any conflicting regulation adopted by a political subdivision.

Proposed law does not allow any person to disclose a trade secret.

A violation of proposed law does not provide a basis for a private cause of action.

Effective Dec. 31, 2023.

(Amends R.S. 44:4.1(B)(35); Adds R.S. 51:1381-1397)

Summary of Amendments Adopted by House

The Committee Amendments Proposed by House Committee on Commerce to the original bill:

1. Modify the definition of "biometric data", "consent", "deidentified data", "identifiable individual", "personal data", "sensitive data", and "specific geolocation data".

2. Remove all references to "pseudonymous data".

3. Create a consumer right to change inaccuracies on a person's data.

4. Add a requirement that controllers conduct a data protection assessment prior to engaging in processing activities that present a heightened risk of harm to a customer.

5. Provide for a public records exception.

6. Make technical changes.

The Committee Amendments Proposed by House Committee on House and Governmental Affairs to the engrossed bill:

1. Make technical changes.