2026 Regular Session **ENROLLED**

SENATE BILL NO. 386

BY SENATORS CONNICK, BARROW, HENRY, JACKSON-ANDREWS, JENKINS, LUNEAU, MILLER, PRICE, SELDERS, STINE AND WOMACK AND REPRESENTATIVE CHASSION

AN ACT

To enact Chapter 20-B of Title 51 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 51:1780.1 through 1780.5, relative to consumer data privacy; creates the Louisiana Data Privacy Act; to provide for limitations and restrictions of the use of certain data; to provide for duties of a controller and processor; to provide for consumer rights regarding personal data; to provide for applicability and exemptions; to provide for public notice; to provide for definitions and terms; to provide for enforcement; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. Chapter 20-B of Title 51 of the Louisiana Revised Statutes of 1950, comprised of R.S. 51:1780.1 through 1780.5, is hereby enacted to read as follows:

**CHAPTER 20-B. LOUISIANA DATA PRIVACY ACT**

**§1780.1. Definitions**

**As used in this Chapter, the following terms have the following meanings:**

**(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For purposes of this Paragraph, "control" or "controlled" means any of the following:**

**(a) The ownership of, or power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company.**

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

**(c) The power to exercise controlling influence over the management of a company.**

**(2) "Authenticate" means to verify through reasonable means that the**

**consumer who is entitled to exercise the consumer's rights pursuant to R.S. 51:1780.3 is the same consumer exercising those consumer rights with respect to the personal data at issue.**

**(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics that are used to identify a specific individual. The term includes a fingerprint, voiceprint, eye retina or iris scan, or other unique biological pattern or characteristic when such data is used to identify the specific individual. The term does not include a physical or digital photograph or data generated from a physical or digital photograph or a video or audio recording or data generated from a video or audio recording, unless such data is generated to identify a specific individual. The term does not include information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(4) "Business associate" has the same meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996, 45 CFR Part 160.103.**

**(5) "Child" means an individual younger than thirteen years of age.**

**(6) "Consent" when referring to a consumer means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. The term does not include any of the following:**

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

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

**(c) Agreement obtained through the use of dark patterns.**

**(7) "Consumer" means an individual who is a resident of this state acting**

**only in an individual or household context. The term does not include an individual acting in a commercial or employment context.**

**(8) "Controller" means an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data.**

**(9) "Covered entity" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(10) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a dark pattern.**

**(11) "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of any of the following:**

**(a) Financial and lending services.**

**(b) Housing, insurance, or healthcare services.**

**(c) Education enrollment.**

**(d) Employment opportunities.**

**(e) Criminal justice.**

**(f) Access to basic necessities, such as food and water.**

**(12) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to an identified or identifiable individual, or a device linked to that individual, if the controller or processor that possesses such data does all of the following:**

**(a) Takes reasonable measures to ensure that such data cannot be associated with an individual.**

**(b) Publicly commits to process such data only in a deidentified fashion and attempt to reidentify such data.**

**(c) Contractually obligates any recipients of such data to satisfy the criteria set forth in Subparagraphs (a) and (b) of this Paragraph.**

**(13) "Healthcare provider" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(14) "Health record" means any written, printed, or electronically recorded material maintained by a healthcare provider in the course of providing healthcare services to an individual that concerns the individual and the services provided. The term includes either one of the following items:**

**(a) The substance of any communication made by an individual to a healthcare provider in confidence during or in connection with the provision of healthcare services.**

**(b) Information otherwise acquired by the healthcare provider about an individual in confidence and in connection with healthcare services provided to the individual.**

**(15) "Identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.**

**(16) "Institution of higher education" means either one of the following items:**

**(a) An institution of higher education as defined by law.**

**(b) A private or independent institution of higher education as defined by law.**

**(17) "Known child" means a child under circumstances where a controller has actual knowledge of, or willfully disregards, the child's age.**

**(18) "Nonprofit organization" means any of the following:**

**(a) A corporation organized under the provisions of Chapter 2 of Title 12 of the Louisiana Revised Statutes of 1950, to the extent applicable to nonprofit corporations.**

**(b) An organization exempt from federal taxation under Section 501(a) of the Internal Revenue Code of 1986, as amended by being listed as an exempt organization under Sections 501(c)(3), 501(c)(6), 501(c)(12), or 501(c)(19) of that Code.**

**(c) A political organization.**

**(d) An organization that is exempt from federal taxation under Section 501(a) of the Internal Revenue Code of 1986, as amended by being listed as an exempt organization under Section 501(c)(4) of that Code.**

**(19) "Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term does not include deidentified data or publicly available information.**

**(20) "Political organization" means a party, committee, association, fund, or other organization, regardless of whether incorporated, that is organized and operated primarily for the purpose of influencing or attempting to influence either of the following:**

**(a) The selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed.**

**(b) The election of a presidential/vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.**

**(c) The outcome of any ballot measure, referendum, initiative, or recall election at the federal, state, or local level.**

**(d) Any political, legislative, or public policy matter, including public opinion relating thereto.**

**(21) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. The term does not include the content of communications, or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.**

**(22) "Process" or "processing" 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.**

**(23) "Processor" means a person that processes personal data on behalf of a controller.**

**(24) "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.**

**(25) "Protected health information" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(26) "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.**

**(27) "Publicly available information" means information that is lawfully made available through government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.**

**(28) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following:**

**(a) The disclosure of personal data to a processor that processes the personal data on the controller's behalf.**

**(b) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer.**

**(c) The disclosure or transfer of personal data to an affiliate of the**

**controller.**

**(d) The disclosure of information that the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience.**

**(e) The disclosure of personal data directed by a consumer or made when the consumer uses the controller to interact with a third party.**

**(f) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, or similar activity, or a proposed merger, acquisition, or similar activity.**

**(29) "Sensitive data" means a category of personal data. The term includes any of the following:**

**(a) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status.**

**(b) Genetic or biometric data that is processed for the purpose of uniquely identifying an individual.**

**(c) Personal data collected from a known child.**

**(d) Precise geolocation data.**

**(30) "State agency" means a department, commission, board, office, council, authority, or other agency in any branch of state government that is created by the constitution or a statute of this state, including a university system or institution of higher education as defined by law.**

**(31) "Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. The term does not include an advertisement that is:**

**(a) Based on activities within a controller's own websites or online applications.**

**(b) Based on the context of a consumer's current search query, visit to**

**a website, or online application.**

**(c) Directed to a consumer in response to the consumer's request for information or feedback.**

**(d) The processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.**

**(32) "Third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor.**

**(33) "Trade secret" means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:**

**(a) The owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret.**

**(b) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.**

**§1780.2. Applicability; preemption**

**A. The provisions of this Chapter shall apply only to a person or entity that does business in the state and that satisfies one or more of the following thresholds:**

**(1) Has annual gross revenues in excess of twenty-five million dollars.**

**(2) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of seventy-five thousand or more consumers, households, or devices.**

**(3) Derives fifty percent or more of its annual revenues from selling consumers' personal information.**

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

**(1) A state agency or a political subdivision of this state.**

**(2) A financial institution and its affiliates or data subject to Title V, Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., and the rules and implementing regulations promulgated thereunder.**

**(3) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, 45 CFR Parts 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(4) A nonprofit organization.**

**(5) An institution of higher education.**

**(6) An electric public utility as defined in R.S. 45:121.**

**(7) A person, association, partnership, or corporation registered with the secretary of state as a conductor of public opinion polls pursuant to R.S. 14:325.**

**C. The following information is exempt from this Chapter:**

**(1) Protected health information under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(2) Health records.**

**(3) Patient identifying information for purposes of 42 U.S.C. 290dd-2.**

**(4) Identifiable private information:**

**(a) For purposes of the federal policy for the protection of human subjects under 45 CFR Part 46.**

**(b) Collected as part of human subjects research under the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, otherwise known as ICH, or of the protection of human subjects under 21 CFR Parts 50 and 56.**

**(c) That is personal data used or shared in research conducted in accordance with the requirements set forth in this Chapter or other research**

**conducted in accordance with applicable law.**

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

**(6) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21 et seq.**

**(7) Information derived from any of the healthcare-related information listed in this Section that is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this Section that is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq., or by a program or a qualified service organization as defined by 42 U.S.C. 290dd-2.**

**(9) Information that is included in a limited data set as described by 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by 45 CFR 164.514(e).**

**(10) Information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.**

**(11) 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 by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.**

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

**(13) Personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g.**

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

**(15) Data processed or maintained 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 that the data is collected and used within the context of that role.**

**(16) Data processed or maintained as the emergency contact information of an individual under this Chapter that is used for emergency contact purposes.**

**(17) Data that is processed or maintained and is necessary to retain to administer benefits for another individual that relates to an individual described by R.S. 51:1780.1(15) and used for the purposes of administering those benefits.**

**D. The provisions of this Chapter shall not apply to the processing of personal data by a person in the course of a purely personal or household activity.**

**E. A controller or processor that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq., and its rules, regulations, and exemptions with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent under this Chapter.**

**§1780.3. Consumer rights; requests; appeals**

**A.(1) A consumer is entitled to exercise the consumer rights authorized by this Section at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise the consumer rights on behalf of the child.**

**(2) A controller shall comply with an authenticated consumer request to**

**exercise the right to do any of the following:**

**(a) Confirm whether a controller is processing the consumer's personal data and to access the personal data.**

**(b) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.**

**(c) Delete personal data provided by or obtained about the consumer.**

**(d) If the data is available in a digital format, obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance.**

**(e) Opt out of the processing of the personal data for purposes of:**

**(i) Targeted advertising.**

**(ii) The sale of personal data.**

**(iii) Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.**

**(3) Nothing in this Section shall require the controller to reveal a trade secret.**

**B.(1) Except as otherwise provided by this Chapter, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to Paragraph (A)(1) of this Section.**

**(2) A controller shall respond to the consumer request without undue delay, which may not be later than the forty-fifth calendar day after the date of receipt of the request. The controller may extend the response period once by an additional forty-five days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five day response period, together with the reason for the extension.**

**(3) If a controller declines to take action regarding the consumer's**

**request, the controller shall inform the consumer without undue delay, which may not be later than the forty-fifth calendar day after the date of receipt of the request, of the justification for declining to take action and provide instructions on how to appeal the decision in accordance with Subsection C of this Section.**

**(4) A controller shall provide information in response to a consumer request free of charge, up to twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The controller bears the burden of demonstrating for purposes of this Subsection that a request is manifestly unfounded, excessive, or repetitive.**

**(5) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a consumer request submitted pursuant to Subsection A of this Section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.**

**(6) A controller that has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete that personal data pursuant to Subparagraph (A)(2)(c) of this Section by either of the following:**

**(a) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using the retained data for any other purpose under this Chapter.**

**(b) Opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this Chapter.**

**C.(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decisions pursuant to Paragraph (B)(3)**

**of this Section.**

**(2) The appeal process shall be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request pursuant to Subsection A of this Section.**

**(3) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this Section not later than the sixtieth calendar day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.**

**(4) If the controller denies an appeal, the controller shall provide the consumer with the online mechanism described by R.S. 51:1780.5(B)(2) through which the consumer may contact the attorney general to submit a complaint.**

**D. Any provision of a contract or agreement that waives or limits in any way a consumer right described in this Section is contrary to public policy and is void and unenforceable.**

**E.(1) A controller shall establish two or more secure and reliable methods to enable consumers to submit a request to exercise their consumer rights under this Chapter. The methods shall take into account all of the following:**

**(a) The ways in which consumers normally interact with the controller.**

**(b) The necessity for secure and reliable communications of those requests.**

**(c) The ability of the controller to authenticate the identity of the consumer making the request.**

**(2) A controller may not require a consumer to create a new account to exercise the consumer's rights under this Chapter but may require a consumer to use an existing account.**

**(3) Except as provided by R.S. 51:1780.1(28)(d), if the controller maintains a website, the controller shall provide a mechanism on the website for consumers to submit requests for information required to be disclosed under this Chapter.**

**(4) A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information is only required to provide an email address for the submission of requests described by Subparagraph(1)(c) of this Subsection.**

**(5) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data pursuant to Items (A)(2)(e)(i) and (ii) of this Section. A consumer may designate an authorized agent using a technology, including a link to a website, an internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing for targeted advertising, for sale of personal data, or both. A controller shall comply with an opt-out request received from an authorized agent under this Subsection if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this Subsection if any one of the following applies:**

**(a) The authorized agent does not communicate the request to the controller in a clear and unambiguous manner.**

**(b) The controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state.**

**(c) The controller does not possess the ability to process the request.**

**(d) The controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.**

**(6) The technology described by this Subsection:**

**(a) Shall not unfairly disadvantage another controller.**

**(b) May not make use of a default setting, but shall require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer's intent to opt out of any processing of a consumer's personal data.**

**(c) Shall be consumer-friendly and easy to use by the average consumer.**

**§1780.4. Duties**

**A.(1) A controller:**

**(a) Shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed to the consumer.**

**(b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue.**

**(2) A controller shall not:**

**(a) Except as otherwise provided by this Chapter, process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.**

**(b) Process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers.**

**(c) Discriminate against a consumer for exercising any of the consumer rights contained in this Chapter, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.**

**(d) Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data in accordance with the rules, regulations, and the exceptions of the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq.**

**(3) This Subsection may not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to**

**a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out pursuant to R.S. 51:1780.3(A) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.**

**B.(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, including, if applicable, any sensitive data processed by the controller.**

**(b) The purpose for processing personal data.**

**(c) A process on how consumers may exercise their consumer rights pursuant to R.S. 51:1780.3, including the process by which a consumer may appeal a controller's decision with regard to the consumer's request.**

**(d) If applicable, the categories of personal data that the controller sells to third parties.**

**(e) If applicable, the categories of third parties with whom the controller sells personal data.**

**(f) A description of the methods required pursuant to R.S. 51:1780.3(E) through which consumers can submit requests to exercise their consumer rights under this Chapter.**

**(2) If a controller engages in the sale of personal data that is sensitive, the controller shall post the following notice in the same manner as the privacy notice described in Subsection B of this Section:**

**"NOTICE: We may sell your sensitive personal data."**

**(3) If a controller engages in the sale of personal data that is biometric data, the controller shall post the following notice in the same manner as the privacy notice described in Subsection B of this Section:**

**"NOTICE: We may sell your biometric personal data."**

**C. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that process and the manner in which a consumer may**

**exercise the right to opt out of that process.**

**D.(1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties or requirements under this Chapter, including:**

**(a) Taking into account the nature of processing and the information available to the processor, by using appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests submitted pursuant to R.S. 51:1780.3(A).**

**(b) Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing personal data, and in relation to the notification of a breach of security of the processor's system pursuant to R.S. 51:3071 et seq.**

**(c) Providing necessary information to enable the controller to conduct and document data protection assessments under Subsection E of this Section.**

**(2) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall include all of the following:**

**(a) Clear instructions for processing data.**

**(b) The nature and purpose of processing.**

**(c) The type of data subject to processing.**

**(d) The duration of processing.**

**(e) The rights and obligations of both parties.**

**(f) A requirement that the processor shall do all of the following:**

**(i) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.**

**(ii) At the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law.**

**(iii) Make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of this Chapter.**

**(iv) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor.**

**(v) Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.**

**(3) Notwithstanding any other provisions of this Chapter, a processor, in the alternative, may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under this Chapter using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller on request.**

**(4) This Section shall not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this Chapter.**

**(5) A determination of 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 on the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.**

**E.(1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:**

**(a) The processing of personal data for purposes of targeted advertising.**

**(b) The sale of personal data.**

**(c) The processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of any of the following:**

**(i) Unfair or deceptive treatment of or unlawful disparate impact on consumers.**

**(ii) Financial, physical, or reputational injury to consumers.**

**(iii) A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person.**

**(iv) Other substantial injury to consumers.**

**(d) The processing of sensitive data.**

**(e) Any processing activities involving personal data that present a heightened risk of harm to consumers.**

**(2) A data protection assessment conducted pursuant to Paragraph (1) of this Subsection shall do both of the following:**

**(a) Identify and weigh the direct or indirect benefits that may flow 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 that processing, as mitigated by safeguards that can be employed by the controller to reduce the risks.**

**(b) Factor into the assessment all of the following:**

**(i) The use of deidentified data.**

**(ii) The reasonable expectations of consumers.**

**(iii) The context of the processing.**

**(iv) The relationship between the controller and the consumer whose personal data will be processed.**

**(3) A controller shall make a data protection assessment requested pursuant to R.S. 51:1780.5(C)(2) available to the attorney general pursuant to a civil investigative demand pursuant to R.S. 51:1780.5(C).**

**(4) A data protection assessment is confidential and exempt from public inspection and copying pursuant to this Section. Disclosure of a data protection assessment in compliance with a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with**

**respect to the assessment and any information contained in the assessment.**

**(5) A single data protection assessment may address a comparable set of processing operations that include similar activities.**

**(6) A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this Section if the assessment has a reasonably comparable scope and effect.**

**(7) Data protection assessments are required for processing activities as of January 1, 2027, and are not retroactive.**

**F.(1) A controller in possession of deidentified data shall do all of the following:**

**(a) Take reasonable measures to ensure that the data cannot be associated with an individual.**

**(b) Publicly commit to maintaining and using deidentified data without attempting to reidentify the data.**

**(c) Contractually obligate any recipient of the deidentified data to comply with the provisions of this Chapter.**

**(2) This Chapter shall not be construed to require a controller or processor to do any of the following:**

**(a) Reidentify deidentified data or pseudonymous data.**

**(b) 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.**

**(c) Comply with an authenticated consumer rights request under R.S. 51:1780.3(A), if the controller is all of the following:**

**(i) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.**

**(ii) Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data**

**with other personal data about the same specific consumer.**

**(iii) Does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted by this Section.**

**G. This Section shall not prevent a controller or processor's ability to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such actions.**

**H. This Chapter shall not be construed to limit a controller or processor's ability to do any of the following:**

**(1) Comply with federal, state, or local laws, rules, or regulations.**

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

**(3) Investigate, establish, exercise, prepare for, or defend legal claims.**

**(4) Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or taking steps at the request of the consumer before entering into a contract.**

**(5) Take immediate steps to protect against an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis.**

**(6) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similarly independent oversight entity that determines all of the following has occurred:**

**(a) If the deletion of the information is likely to provide benefits that do not exclusively accrue to the controller.**

**(b) Whether the expected benefits of the research outweigh the privacy risks.**

**(c) If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.**

**(7) Assist another controller, processor, or third party with any of the requirements pursuant to this Subsection.**

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

**I. The obligations imposed on controllers or processors pursuant to this Chapter shall not restrict a controller's or processor's ability to collect, use, or retain data for internal use to do any of the following:**

**(1) Conduct internal research to develop, improve, or repair products, service, or technology.**

**(2) Effectuate a product recall.**

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

**(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provisions of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.**

**J. The obligations imposed on controllers or processors pursuant to this Chapter shall not apply where compliance by the controller or processor with said Sections would violate an evidentiary privilege pursuant to the laws of this state. Nothing in this Chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege pursuant to the laws of the state as part of**

**a privileged communication.**

**K. Nothing in this Chapter shall be construed to impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including but not limited to the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution.**

**L.(1) Personal data processed by a controller pursuant to this Section may be processed to the extent that such processing is both of the following:**

**(a) Reasonably necessary and proportionate to the purposes listed in this Section.**

**(b) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this Section.**

**(2) Personal data collected, used, or retained pursuant to Subsection I of this Section shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.**

**M. If a controller processes personal data pursuant to an exemption in this Section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in Subsection L of this Section.**

**N. Processing personal data for the purposes expressly identified in Subsections G through I of this Section shall not solely make a legal entity a controller with respect to such processing.**

**O.(1) The consumer rights pursuant to R.S. 51:1780.3(A)(2)(a) through (e) and controller duties pursuant to this Section do not apply to pseudonymous data in cases in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective**

**technical and organizational controls that prevent the controller from accessing the information.**

**(2) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breach of the contractual commitments.**

**P.(1) A person or entity described by R.S. 51:1780.2(A)(3) may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer.**

**(2) A person who violates this Section is subject to the penalty under R.S. 51:1780.5.**

**§1780.5. Enforcement**

**A. The attorney general shall enforce the provisions of this Chapter.**

**B. The attorney general shall post on his website, information relating to the responsibilities of a controller and a processor and consumer rights pursuant to this Chapter.**

**C. Any violation of the provisions of this Chapter shall constitute an unfair and deceptive trade practice pursuant to the Unfair Trade Practices and Consumer Protection Law, R.S. 51:1401 et seq., excluding private rights of action as provided in R.S. 51:1409 and 1409.1. Notwithstanding any other provision of law to the contrary, any monies received related to the attorney general's enforcement of this Chapter shall be used by the attorney general for consumer protection efforts or to promote consumer protection and education.**

**D. Beginning January 1, 2027, and ending July 31, 2027, before bringing an action pursuant to this Section, the attorney general shall notify a person in writing, not later than the thirtieth calendar day before initiating an investigation, identifying the specific provisions of this Chapter the attorney general alleges is being violated. The attorney general shall not initiate an investigation against the person if the person does all of the following:**

**(1) Cures the alleged violation identified by the attorney general within the thirty-day period.**

**(2) Provides the attorney general with a written statement that the person cured the alleged violation.**

**(3) Submits supportive documentation to the attorney general to show how the privacy violation was cured.**

**(4) Changes are made to the internal policy, if necessary, to ensure that no such further violations occur.**

Section 2. This Act shall become effective on January 1, 2027.

_____
PRESIDENT OF THE SENATE

_____
SPEAKER OF THE HOUSE OF REPRESENTATIVES

_____
GOVERNOR OF THE STATE OF LOUISIANA

APPROVED: _____