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)]

SB 386 Reengrossed 2026 Regular Session Connick

Proposed law creates the Louisiana Data Privacy Act.

Proposed law provides for definitions and terms.

Proposed law provides that proposed law applies only to a person that does business in the state and meets one or more specified thresholds, including annual gross revenues exceeding $25 million, processing the personal data of 75,000 or more consumers, households, or devices, or deriving 50% or more of annual revenues from the sale of personal data.

Proposed law exempts state agencies, political subdivisions, financial institutions, nonprofit organizations, institutions of higher education, electric public utilities, and entities governed by the privacy and security rules from proposed law.

Proposed law provides that certain information is exempt from proposed law.

Proposed law excludes personal or household activities from the applicability of proposed law and requires a controller or processor to use verifiable parental consent with respect to data collection online pursuant to federal law.

Proposed law allows a consumer, or a parent or legal guardian of a known child, to submit a request to a controller to confirm and access personal data, correct inaccuracies, delete personal data, obtain a portable copy of previously provided data, and opt out of targeted advertising, sale of personal data, or certain profiling.

Proposed law requires a controller to respond to a consumer's request within 45 days, or extended once for 45 days, and to provide notice, justification, and appeal instructions if a request is denied. Proposed law allows up to two free responses annually and permits reasonable fees for administrative costs for manifestly unfounded, excessive, or repetitive requests.

Proposed law provides that if a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a consumer request.

Proposed law provides methods by which a controller may comply with deletion requests for data obtained from a source other than the consumer.

Proposed law requires a controller to establish a process for appeal and to respond to appeals within 60 days, and if denied, the controller must provide a mechanism for the consumer to submit a complaint to the attorney general.

Proposed law provides that any contractual provision waiving or limiting a consumer's right is against public policy and is void and unenforceable.

Proposed law requires a controller to establish at least two secure and reliable methods for consumers to submit requests to exercise their rights, taking certain information into account.

Proposed law prohibits a controller from requiring a consumer to create a new account to exercise rights. Requires a website mechanism for submitting requests if the controller maintains a website. Requires exclusively online controller with a direct consumer relationship to provide only an email address for submission of requests.

Proposed law allows a consumer to designate an authorized agent, including through technology-based opt-out signals such as a browser setting or device-level signals, to act on the consumer's behalf for opt-out requests.

Proposed law provides for when a controller is nor required to comply with an opt out request received from an authorized agent.

Proposed law provides that technology used by a consumer to designate an authorized agent or communicate an opt-out request shall not unfairly disadvantage a controller.

Proposed law requires that such technology not rely on a default setting and instead require an affirmative, freely given, and unambiguous choice by the consumer to opt out of the processing of personal data. Further requires that the technology be consumer friendly and easy to use.

Proposed law requires a controller to limit collection of personal data to what is adequate, relevant, and reasonably necessary for disclosed purposes and to maintain reasonable administrative, technical, and physical safeguards appropriate to the volume and nature of the data.

Proposed law prohibits a controller from processing personal data for purposes incompatible with disclosed purposes without consumer consent, processing data in violation of state and federal law, discriminating against a consumer for exercising any of the consumer rights outlined in proposed law, and processing the sensitive data of a consumer without obtaining the consumer's consent.

Proposed law clarifies that a controller is not required to provide goods or services that require personal data it does not collect or maintain and may offer different prices, rates, or benefits in connection with a consumer's opt-out or participation in a loyalty or rewards program.

Proposed law requires a controller to provide consumers with a reasonably accessible and clear privacy notice. Provides that the notice must disclose the categories of personal data processed, including sensitive data, the purpose for processing, the process for exercising consumer rights and appealing decisions, the categories of personal data that the controller sells to third parties, the categories of third parties with whom the controller sells personal data, and the methods available for submitting consumer rights requests.

Proposed law requires that a controller engaging in the sale of sensitive personal data and the sale of biometric personal data post a conspicuous notice.

Proposed law requires that if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing and provide notice of the manner in which a consumer may exercise the right to opt out.

Proposed law requires a processor to adhere to the instructions of a controller and to assist the controller in complying with duties under proposed law.

Proposed law requires that processing performed by a processor on behalf of a controller be governed by a written contract with specific requirements. Further allows a processor to obtain an independent assessment using an accepted control standard or framework and to provide the report to the controller upon request.

Proposed law clarifies that proposed law does not relieve either a controller or processor of liability arising from its respective role under proposed law. Further provides that when a person is acting as a controller or processor is determined by a fact-based analysis of the specific processing context and that a processor remains a processor so long as it adheres to the controller's instructions.

Proposed law requires a controller to conduct and document a data protection assessment for specified processing activities. Further provides for what shall be included in the data protection assessment.

Proposed law requires a controller to provide a data protection assessment that shall be confidential and exempt from public records disclosure to the attorney general upon request pursuant to a civil investigative demand.

Proposed law provides that a single data protection assessment may address a comparable set of processing operations that include similar activities and are conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of proposed law if the assessment has a reasonably comparable scope and effect.

Proposed law requires controllers possessing deidentified data to take reasonable measures to prevent reidentification, publicly commit not to reidentify the data, and obligate recipients to comply with proposed law.

Proposed law provides that controllers and processors are not required to reidentify data, maintain data in identifiable form, or comply with certain consumer requests when the data cannot reasonably be linked to a specific consumer, does not use the personal data to recognize or respond to the specific customer, and is not sold or disclosed.

Proposed law provides that proposed law shall not prevent a controller or processor from preventing, detecting, protecting against, or responding to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity, or from preserving system integrity or investigating, reporting, or prosecuting such conduct.

Proposed law provides for when consumer rights and controller duties pursuant to proposed law shall not apply. Proposed law requires reasonable oversight of deidentified or pseudonymous data in certain circumstances.

Proposed law provides that proposed law shall not be construed to limit a controller or processor's ability to take certain actions.

Proposed law provides that the obligations imposed on controllers or processors pursuant to proposed law shall not restrict a controller's or processor's ability to collect, use, or retain data for internal use to take certain actions.

Proposed law provides that the obligations imposed on controllers or processors pursuant to proposed law shall not apply where compliance by the controller or processor would violate an evidentiary privilege pursuant to the laws of this state.

Proposed law provides that nothing in proposed law shall be construed to impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person.

Proposed law allows for certain personal data processed by a controller to be processed to the extent that such processing is reasonably necessary and proportionate to the purposes listed in proposed law and is adequate, relevant, and limited to what is necessary in relation to specific purposes.

Proposed law provides that personal data collected, used, or retained pursuant to proposed law shall 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.

Proposed law requires that if a controller processes personal data pursuant to an exemption in proposed law, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in proposed law.

Proposed law provides that processing personal data for the purposes expressly identified in proposed law shall not solely make a legal entity a controller with respect to such processing.

Proposed law prohibits the sale of sensitive personal data without prior consumer consent.

Proposed law authorizes the attorney general to enforce the provisions of proposed law.

Proposed law requires the attorney general to post on its website information regarding the responsibilities of controllers and processors and consumer rights.

Proposed law provides that a violation under proposed law constitutes an unfair and deceptive trade practice. Further, excludes a private right of action, and requires that any monies received from enforcement by the attorney general be used for consumer protection and education efforts.

Proposed law requires the attorney general beginning January 1, 2027, and ending July 21, 2027, to provide written notice of an alleged violation at least 30 calendar days prior to initiating an investigation. Further provides that the attorney general shall not initiate an investigation if the person cures the violation by providing written certification and supporting documentation of the cure, and makes necessary internal policy changes to prevent future violations.

Effective January 1, 2027.

(Adds R.S. 51:1776-1780)

Summary of Amendments Adopted by Senate

Committee Amendments Proposed by Senate Committee on Commerce, Consumer Protection, and International Affairs to the original bill

1. Limits applicability of proposed law to persons that do business in the state and meet specified revenue or data-processing thresholds.

2. Adds an exception allowing controllers and processors to take necessary actions to prevent and respond to fraud, security threats, and illegal activity and to protect system integrity.

3. Creates an unfair trade practice for any violations of proposed law and provide for enforcement by the attorney general.

4. Establishes a temporary cure period before enforcement of proposed law.

5. Removes provisions authorizing the attorney general to bring civil action for penalties.

6. Eliminates the private right of action for consumers.

7. Makes effective date January 1, 2027.

8. Makes technical changes.

Senate Floor Amendments to engrossed bill

1. Makes technical changes.

Summary of Amendments Adopted by House

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

1. Make technical changes.

2. Amend the definitions of "biometric data", "deidentified data", "personal data", "political organization", "sale of personal data", and "targeted advertising".

3. Clarify an exemption of proposed law.

4. Clarify when a controller or processor complies with federal law.

5. Clarify a consumer right that the controller shall comply with.

6. Clarify that a consumer may designate an authorized agent using a technology that allows the consumer to indicate the consumer's intent to opt out of the processing for targeted advertising, for the sale of personal data, or both.

7. Clarify proposed law relative to a controller processing data pursuant to federal law.

8. Amend what information shall be included by a controller in a reasonably accessible and clear privacy notice.

9. Amend how 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 pursuant to proposed law.

10. Add that data protection assessments are required for processing activities as of the effective date of proposed law and are not retroactive.

11. Add that proposed law shall not be construed to limit a controller or processor's ability to take certain actions.

12. Add that the obligations imposed on controllers or processors pursuant to proposed law shall not restrict a controller's or processor's ability to collect, use, or retain data for internal use to take certain actions.

13. Add that the obligations imposed on controllers or processors pursuant to proposed law shall not apply where compliance by the controller or processor would violate an evidentiary privilege pursuant to the laws of this state.

14. Add that nothing in proposed law shall be construed to impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person.

15. Add that certain personal data processed by a controller can be processed to the extent that such processing is reasonably necessary and proportionate to the purposes listed in proposed law and is adequate, relevant, and limited to what is necessary in relation to specific purposes.

16. Add that personal data collected, used, or retained pursuant to proposed law shall take into account the nature and purpose or purposes of such collection, use, or retention. Further provide for what such data shall be subject to.

17. Add that if a controller processes personal data pursuant to an exemption in proposed law, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in proposed law.

18. Add that processing personal data for the purposes expressly identified in proposed law shall not solely make a legal entity a controller with respect to such processing.

19. Remove proposed law relative to notifying the consumer that the consumer's privacy violation was addressed provided the consumer's contact information has been made available to the person.