2024 Regular Session

HOUSE BILL NO. 947

BY REPRESENTATIVE DAVIS

CONSUMERS/PROTECTION: Provides relative to the protection of data

1   AN ACT

2   To amend and reenact R.S. 44:4.1(B)(35) and to enact Chapter 12-B of Title 51 of the

3   Louisiana Revised Statutes of 1950, to be comprised of R.S. 51:1381 through 1397,

4   relative to data privacy; to provide definitions; to provide for applicability; to

5   provide for consumer rights; to require a response to a request; to provide for the

6   responsibilities of a processor and a controller; to provide for deidentified data; to

7   provide for limitations; to provide for investigative powers; to provide for

8   enforcement; to provide for a civil fine; to provide for a data assessment; to provide

9   for a public records exception; to create an account; to require a report; to provide

10   for an effective date; and to provide for related matters.

11   Be it enacted by the Legislature of Louisiana:

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

13   §4.1. Exceptions

14   *   *   *

15   B. The legislature further recognizes that there exist exceptions, exemptions,

16   and limitations to the laws pertaining to public records throughout the revised

17   statutes and codes of this state. Therefore, the following exceptions, exemptions, and

18   limitations are hereby continued in effect by incorporation into this Chapter by

19   citation:

20   *   *   *

1   (35) R.S. 51:710.2(B), 705, 706, 936, 1363.1, 1395, 1404, 1926, 1934, 2113,

2   2182, 2262, 2318, 2370.3, 2370.16, 2370.25, 2370.27, 2389

3   *   *   *

4   Section 2. Chapter 12-B of Title 51 of the Louisiana Revised Statutes of 1950,

5 comprised of R.S. 51:1381 through 1397, is hereby enacted to read as follows:

6   CHAPTER 12-B. LOUISIANA CONSUMER PRIVACY ACT

7   §1381. Short title

8   This Chapter shall be known and may be cited as the "Louisiana Consumer

9 Privacy Act".

10   §1382. Definitions

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

12   (1) "Account" means the consumer privacy restricted account established in

13 R.S. 51:1396.

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

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

16 entity.

17   (b) Shares common branding with another entity.

18   (3) "Aggregated data" means information that relates to a group or category

19 of consumers that satisfies all of the following criteria:

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

21 information.

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

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

24   (5) "Authenticate" means to use reasonable means to determine that a

25 consumer's request to exercise the rights described in R.S. 51:1385 is made by the

26 consumer who is entitled to exercise those rights.

27   (6)(a) "Biometric data" means data generated by automatic measurements

28 of an individual's unique physical, physiological, or biological characteristics that

29 allow or confirm the unique identity of a specific individual.

1   (b) "Biometric data" includes data described in Subparagraph (a) of this

2   Paragraph that is generated by automatic measurements of an individual's fingerprint,

3   voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic

4   that is used to identify a specific individual.

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

6   (i) A physical or digital photograph.

7   (ii) A video or audio recording.

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

9   (iv) Information collected, used, or stored for treatment, payment, or

10   healthcare operations as those terms are defined in 45 CFR Parts 160, 162, and 164.

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

12   160.103.

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

14   (9)(a) "Consent" means a clear and affirmative act by a consumer that

15   unambiguously indicates the consumer's voluntary, specific, and informed agreement

16   to allow a person to process personal data related to the consumer.

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

18   (i) Acceptance of general or broad terms of use or a similar document that

19   contains descriptions of personal data processing along with other unrelated

20   information.

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

22   (10)(a) "Consumer" means an individual who is a resident of this state acting

23   in an individual or household context.

24   (b) "Consumer" does not include an individual acting in an employment or

25   commercial context.

26   (11) "Control" or "controlled" as used in Paragraph (2) of this Section means

27   any of the following:

28   (a) Ownership of, or the power to vote with, more than fifty percent of the

29   outstanding shares of any class of voting securities of an entity.

1   (b) Control in any manner over the election of a majority of the directors or

2   of the individuals exercising similar functions.

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

4   entity.

5   (12) "Controller" means a person doing business in this state who determines

6   the purposes for and the means by which personal data is processed, regardless of

7   whether the person makes the determination alone or with others.

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

9   160.103.

10   (14) "Deidentified data" means data that satisfies all of the following criteria:

11   (a) Cannot reasonably be used to infer information about, or otherwise be

12   linked to, an identified individual, device, or household.

13   (b) Is possessed by a controller who does all of the following:

14   (i) Takes reasonable measures to ensure that a person cannot associate the

15   data with an individual.

16   (ii) Publicly commits to maintain and use the data only in its deidentified

17   form and further commits to not attempt to reidentify the data.

18   (iii) Contractually obligates any recipients of the data to comply with the

19   requirements described in this Subparagraph.

20   (15) "Director" means the director of the consumer protection section of the

21   Department of Justice.

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

23   of Justice.

24   (17) "Governmental entity" means any board, authority, commission,

25   department, office, division, or agency of this state or any of its local political

26   subdivisions.

27   (18) "Healthcare facility" means an institution providing medical services

28   or a healthcare setting, including but not limited to a hospital or other licensed

29   inpatient center, an ambulatory surgical or treatment center, a skilled nursing center,

1   a residential treatment center, a rehabilitation center, and a diagnostic, laboratory, or

2   imaging center.

3   (19) "Healthcare provider" means any person licensed, certified, or

4   registered in this state to provide healthcare services, including but not limited to

5   physicians, hospitals, home health agencies, chiropractors, pharmacies, and dentists.

6   (20) "Identified individual" or "identifiable individual" means an individual

7   who can be readily identified, either directly or indirectly, in particular or by

8   reference to an identifier such as a name, an identification number, specific

9   geolocation data, or an online identifier.

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

11   of higher education.

12   (22) "Local political subdivision" means a parish, municipality, and any

13   other unit of local government, including but not limited to a school board or a

14   special district, authorized by law to perform governmental functions.

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

16   (a) A corporation incorporated in accordance with the laws of this state and

17   subject to the provisions of the Nonprofit Corporation Law, R.S. 12:201 et seq.

18   (b) A corporation incorporated in accordance with the laws of another state

19   that would be considered a nonprofit corporation if it were incorporated in

20   accordance with the laws of this state.

21   (24)(a) "Personal data" means information that is linked or reasonably

22   linkable to an identified individual or an identifiable individual.

23   (b) "Personal data" does not include deidentified data and publically

24   available information.

25   (25) "Process" means an operation or set of operations performed on

26   personal data, including but not limited to collection, use, storage, disclosure,

27   analysis, deletion, or modification of personal data.

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

29   a controller.

1   (27) "Protected health information" means the same as that term is defined

2   in 45 CFR 160.103.

3   (28) "Publicly available information" means information that satisfies any

4   of the following criteria:

5   (a) Is lawfully obtained by a person from a record of a governmental entity.

6   (b) Is obtained by a person who reasonably believes a consumer or a widely-

7   distributed media source has lawfully made available to the general public.

8   (c)   Is obtained from a person to whom the consumer disclosed the

9   information, if the consumer has not restricted the information to a specific audience.

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

11   (30)(a) "Sale", "sell", or "sold" means the exchange of personal data for

12   monetary or other valuable consideration by a controller to a third party.

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

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

15   personal data on behalf of the controller.

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

17   (iii) Considering the context in which the consumer provided the personal

18   data to the controller, a controller's disclosure of personal data to a third party if the

19   purpose is consistent with a consumer's reasonable expectations.

20   (iv)   The disclosure or transfer of personal data if a consumer directs a

21   controller to do either of the following:

22   (aa) Disclose the personal data.

23   (bb) Interact with one or more third parties.

24   (v) A consumer's disclosure of personal data to a third party for the purpose

25   of providing a product or service requested by the consumer or a parent or legal

26   guardian of a child.

27   (vi)   The disclosure of information, if the consumer satisfies all of the

28   following criteria:

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

2   media.

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

4   (vii) A controller's transfer of personal data to a third party as an asset that

5   is part of a proposed or actual merger, an acquisition, or a bankruptcy in which the

6   third party assumes control of all or part of the controller's assets.

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

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

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

10   (bb) An individual's religious beliefs.

11   (cc) An individual's sex.

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

13   (ee) Information regarding an individual's medical history, mental or

14   physical health condition, or medical treatment or diagnosis by a healthcare

15   professional.

16   (ii) The processing of genetic personal data or biometric data, if the

17   processing is for the purpose of identifying a specific individual.

18   (iii) Specific geolocation data.

19   (iv) Biometric data.

20   (b) "Sensitive data" does not include personal data that reveals any of the

21   following, if processed in the manner provided:

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

23   communication service.

24   (ii) Any information regarding an individual's medical history, mental or

25   physical health condition, or medical treatment or diagnosis by a healthcare

26   professional, if the personal data is processed by a person licensed to provide health

27   care in accordance with the laws of this state.

28   (32)(a) "Specific geolocation data" means information derived from

29   technology, including global positioning system level latitude and longitude

1 coordinates, that directly identifies an individual's specific location, accurate within

2 a radius of one thousand eight hundred fifty feet or fewer.

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

4 (i) The content of a communication.

5 (ii) Any data generated by or connected to advanced utility metering

6 infrastructure systems or equipment for use by a utility.

7 (33)(a) "Targeted advertising" means displaying an advertisement to a

8 consumer where the advertisement is selected based on personal data obtained from

9 the consumer's activities over time and across nonaffiliated websites or online

10 applications to predict the consumer's preferences or interests.

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

12 (i) Advertising based on a consumer's activities within a controller's website

13 or online application or any affiliated website or online application.

14 (ii) Advertising based on the context of a consumer's current search query

15 or visit to a website or online application.

16 (iii) Advertising directed to a consumer in response to the consumer's request

17 for information, products, services, or feedback.

18 (iv) Processing personal data solely to measure or report on advertising

19 performance, advertising reach, or advertising frequency.

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

21 (a) The consumer, controller, or processor.

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

23 (35) "Trade secret" means information, including a formula, pattern,

24 compilation, program, device, method, technique, or process that satisfies all of the

25 following criteria:

26 (a) Derives independent economic value, actual or potential, from not being

27 generally known or readily ascertainable by proper means by other persons who can

28 obtain economic value from the information's disclosure or use.

1   (b) Is the subject of efforts that are reasonable under the circumstances to

2   maintain the information's secrecy.

3   §1383. Applicability

4   A. The provisions of this Chapter apply to any controller or processor who

5   conducts business in this state or produces a product or service that is targeted to

6   consumers who are residents of this state who satisfy both of the following:

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

8   (2) Satisfies any of the following criteria:

9   (a) During a calendar year, controls or processes the personal data of at least

10   one hundred thousand consumers.

11   (b) Derives over fifty percent of the entity's gross revenue from the sale of

12   personal data and controls or processes the personal data of twenty-five thousand or

13   more consumers.

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

15   (1) A governmental entity or a third party under contract with a

16   governmental entity when the third party is acting on behalf of the governmental

17   entity.

18   (2) A tribe.

19   (3) An institution of higher education.

20   (4) A nonprofit corporation.

21   (5) A covered entity.

22   (6) A business associate.

23   (7) Protected health information for purposes of the Health Insurance

24   Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq. and related

25   regulations.

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

27   (9) Identifiable private information for purposes of the Federal Policy for the

28   Protection of Human Subjects, 45 CFR Part 46.

1   (10) Identifiable private information or personal data collected as part of

2   human subjects research pursuant to or under the same standards as either of the

3   following:

4   (a) The good clinical practice guidelines issued by the International Council

5   for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

6   (b) The Protection of Human Subjects as provided in 21 CFR Part 50 and

7   Institutional Review Boards as provided in 21 CFR Part 56.

8   (11) Personal data used or shared in research conducted in accordance with

9   one or more of the requirements described in Paragraph (9) of this Subsection.

10   (12) Information and documents created specifically for, and collected and

11   maintained by the Louisiana Department of Health.

12   (13) Information and documents created for purposes of the Health Care

13   Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq., and related regulations.

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

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

16   (a) Deidentified in accordance with the requirements for deidentification set

17   forth in 45 CFR Part 164.

18   (b)   Derived from any of the healthcare-related information listed in

19   Paragraphs (7) through (14) of this Subsection.

20   (16) Information originating from or indistinguishably intermingled with

21   information provided for in Paragraphs (7) through (14) of this Subsection that is

22   maintained by either of the following:

23   (a) A healthcare facility or healthcare provider.

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

25   (17)   Information used only for public health activities and purposes as

26   described in 45 CFR 164.512.

27   (18)(a) An activity by any of the following, if all of the criteria provided in

28   Subparagraphs (b) and (c) of this Paragraph are satisfied:

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

1   (ii) A furnisher of information, as set forth in 15 U.S.C. 1681s-2, who

2   provides information for use in a consumer report, as defined in 15 U.S.C. 1681a.

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

4   (b) The activity is subject to regulation under the federal Fair Credit

5   Reporting Act, 15 U.S.C. 1681 et seq.

6   (c) The activity involves the collection, maintenance, disclosure, sale,

7   communication, or use of any personal data that bears on any of the following

8   relative to the consumer:

9   (i) Credit worthiness.

10   (ii) Credit standing.

11   (iii) Credit capacity.

12   (iv) Character.

13   (v) General reputation.

14   (vi) Personal characteristics.

15   (vii) Mode of living.

16   (19) A financial institution or an affiliate of a financial institution governed

17   by, or personal data collected, processed, sold, or disclosed in accordance with, Title

18   V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq. and related regulations.

19   (20) Personal data collected, processed, sold, or disclosed in accordance with

20   the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.

21   (21) Personal data regulated by the Family Education Rights and Privacy

22   Act, 20 U.S.C. 1232g and related regulations.

23   (22) Personal data collected, processed, sold, or disclosed in accordance with

24   the Farm Credit Act of 1971, 12 U.S.C. 2001 et seq.

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

26   (a) In the course of an individual applying to, being employed by, or acting

27   as an agent or independent contractor of a controller, processor, or third party, to the

28   extent the collection and use of the data are related to the individual's role.

1   (b) As the emergency contact information of an individual described in

2   Subparagraph (a) of this Paragraph and used for emergency contact purposes.

3   (c) To administer benefits for another individual relating to an individual

4   described in Subparagraph (a) of this Paragraph and used for the purpose of

5   administering the benefits.

6   (24) An individual's processing of personal data for purely personal or

7   household purposes.

8   (25) An air carrier.

9   C. A controller is in compliance with any obligation to obtain parental

10   consent pursuant to this Chapter if the controller complies with the verifiable

11   parental consent mechanisms as provided in the Children's Online Privacy Protection

12   Act, 15 U.S.C. 6501 et seq. and the act's implementing regulations and exemptions.

13   D. This Chapter does not require a person to take any action in conflict with

14   the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d

15   et seq. or related regulations.

16   §1384. Preemption

17   A. The provisions of this Chapter supersede and preempt any ordinance,

18   resolution, rule, or other regulation adopted by a local political subdivision regarding

19   the processing of personal data by a controller or processor.

20   B. Any reference to federal law in this Chapter includes any rules or

21   regulations promulgated pursuant to that federal law.

22   §1385. Consumer rights

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

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

25   (2) Access the consumer's personal data.

26   (3) Obtain a copy or accurate summary of the consumer's personal data that

27   the consumer provided to the controller within the twelve months preceding the

28   consumer's request, in a format that satisfies all of the following:

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

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

2   (c) Allows the consumer to transmit the data to another controller without

3   impediment, if the processing is carried out by automated means.

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

5   (5) Delete the consumer's personal data that the consumer provided to the

6   controller.

7   (6) Opt out of the processing of the consumer's personal data for either of the

8   following purposes:

9   (a) Targeted advertising.

10   (b) The sale of personal data.

11   B. Nothing in this Section requires a person to cause a breach of a security

12   system as defined in R.S. 51:3073.

13   §1386. Exercising consumer rights

14   A. A consumer may exercise a right provided for in R.S. 51:1385 by

15   submitting a request to a controller, by means prescribed by the controller,

16   specifying the right the consumer intends to exercise.

17   B. In the case of processing personal data concerning a known child, the

18   parent or legal guardian of the known child shall exercise a right on the child's

19   behalf.

20   C. In the case of processing personal data concerning a consumer subject to

21   a guardianship, conservatorship, or other protective arrangement, the guardian or the

22   conservator of the consumer shall exercise a right on the consumer's behalf.

23   §1387. Controller's response to request

24   A. Subject to the other provisions of this Chapter, a controller shall comply

25   with a consumer's request to exercise a right pursuant to R.S. 51:1386.

26   B.(1) Within forty-five days of receiving a request to exercise a right, the

27   controller shall do both of the following:

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

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

1   (2)   The controller may extend the initial forty-five-day period by an

2   additional forty-five days, if reasonably necessary due to the complexity of the

3   request or the volume of the requests received by the controller. The controller may

4   extend the period only once.

5   (3) If a controller extends the initial forty-five-day period, before the initial

6   forty-five-day period expires, the controller shall do all of the following:

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

8   extension.

9   (b) Provide the reasons the extension is reasonably necessary as described

10   in Paragraph (2) of this Subsection.

11   (4)   The forty-five-day period does not apply if the controller reasonably

12   suspects the consumer's request is fraudulent, and the controller is not able to

13   authenticate the request before the forty-five-day period expires.

14   (5) If, in accordance with the provisions of this Section, a controller chooses

15   not to take action on a consumer's request, the controller shall, within forty-five days

16   after the day on which the controller receives the request, inform the consumer of the

17   reasons for not taking action.

18   C.(1) A controller may not charge a fee for information in response to a

19   request, unless the request is the consumer's second or subsequent request during the

20   same twelve-month period.

21   (2)(a) Notwithstanding Paragraph (1) of this Subsection, a controller may

22   charge a reasonable fee to cover the administrative costs of complying with a request

23   or may refuse to act on a request, if any of the following is true:

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

25   unfounded.

26   (ii) The controller reasonably believes the consumer's primary purpose in

27   submitting the request was something other than exercising a right.

28   (iii)   The request, individually or as part of an organized effort, harasses,

29   disrupts, or imposes an undue burden on the resources of the controller's business.

1   (b) A controller who charges a fee or refuses to act in accordance with this

2   Subsection bears the burden of demonstrating the request satisfied one or more of the

3   criteria described in Subparagraph (C)(2)(a) of this Subsection.

4   D. If a controller is unable to authenticate a consumer request to exercise a

5   right described in R.S. 51:1385 using commercially-reasonable efforts, the controller

6   is not required to comply with the request and may request that the consumer provide

7   additional information reasonably necessary to authenticate the request.

8   §1388. Responsibility according to role

9   A. A processor shall do both of the following:

10   (1) Adhere to the controller's instructions.

11   (2)   Taking into account the nature of the processing and information

12   available to the processor, by appropriate technical and organizational measures,

13   insofar as reasonably practicable, assist the controller in meeting the controller's

14   obligations, including obligations related to the security of processing personal data

15   and notification of a breach of a security system described in R.S. 51:3073.

16   B.   Before a processor performs processing on behalf of a controller, the

17   processor and controller shall enter into a contract that satisfies all of the following

18   criteria:

19   (1) Clearly sets forth instructions for processing personal data, the nature and

20   purpose of the processing, the type of data subject to processing, the duration of the

21   processing, and the parties' rights and obligations.

22   (2) Requires the processor to ensure each person processing personal data

23   is subject to a duty of confidentiality with respect to the personal data.

24   (3) Requires the processor to engage any subcontractor pursuant to a written

25   contract that requires the subcontractor to meet the same obligations as the processor

26   with respect to the personal data.

27   C.(1) Determining whether a person is acting as a controller or processor

28   with respect to a specific processing of data is a fact-based determination that

29   depends upon the context in which personal data is to be processed.

1   (2) A processor that adheres to a controller's instructions with respect to a

2   specific processing of personal data remains a processor.

3   §1389. Responsibilities of controllers

4   A.(1) A controller shall provide consumers with a reasonably accessible and

5   clear privacy notice that includes all of the following:

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

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

8   (c) How consumers may exercise a right.

9   (d) The categories of personal data that the controller shares with third

10   parties, if any.

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

12   personal data.

13   (2) If a controller sells a consumer's personal data to one or more third

14   parties or engages in targeted advertising, the controller shall clearly and

15   conspicuously disclose to the consumer the manner in which the consumer may

16   exercise the right to opt out of each of the following:

17   (a) Processing for targeted advertising.

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

19   B.(1) A controller shall establish, implement, and maintain reasonable

20   administrative, technical, and physical data security practices designed to satisfy all

21   of the following criteria:

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

23   (b) Reduce reasonably foreseeable risks of harm to consumers relating to the

24   processing of personal data.

25   (2) Considering the controller's business size, scope, and type, a controller

26   shall use data security practices that are appropriate for the volume and nature of the

27   personal data at issue.

1   C. Except as otherwise provided for in this Chapter, a controller shall not

2   process sensitive data collected from a consumer without doing either of the

3   following:

4   (1) Presenting the consumer with clear notice and an opportunity to opt out

5   of the processing, prior to the data being processed.

6   (2) Processing the data in accordance with the Children's Online Privacy

7   Protection Act, 15 U.S.C. 6501 et seq., and the act's implementing regulations and

8   exemptions, in the case of the processing of personal data concerning a known child.

9   D.(1) A controller may not discriminate against a consumer for exercising

10   a right by doing any of the following:

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

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

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

14   (2) This Subsection does not prohibit a controller from offering a different

15   price, rate, level, quality, or selection of a good or service to a consumer, including

16   offering a good or service for no fee or at a discount, if either of the following is true:

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

18   (b) The offer is related to the consumer's voluntary participation in a bona

19   fide loyalty, rewards, premium features, discounts, or club card program.

20   E.   Notwithstanding the provisions of Subsection D of this Section, a

21   controller is not required to provide a product, service, or functionality to a consumer

22   if all of the following are satisfied:

23   (1) The consumer's personal data is or the processing of the consumer's

24   personal data is reasonably necessary for the controller to provide the consumer the

25   product, service, or functionality.

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

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

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

1   F. Any provision of a contract that purports to waive or limit a consumer's

2   right in accordance with this Chapter is absolutely null.

3   §1390. Processing deidentified data

4   A. A controller of deidentified data shall:

5   (1) Take reasonable measures to ensure that a person cannot associate the

6   data with an individual.

7   (2) Publicly commit to maintain and use the data only in its deidentified

8   form and to not attempt to reidentify the data.

9   (3) Contractually obligate any recipient of the data to comply with the

10   requirements of this Subsection.

11   B. The provisions of this Chapter do not require a controller or processor to

12   do any of the following:

13   (1) Reidentify deidentified data.

14   (2) Maintain data in identifiable form or obtain, retain, or access any data or

15   technology for the purpose of allowing the controller or processor to associate a

16   consumer request with personal data.

17   (3)(a) Comply with an authenticated consumer request to exercise a right as

18   described in R.S. 51:1386, if the controller complies with Subparagraph (b) of this

19   Paragraph and either of the following is satisfied:

20   (i) The controller is not reasonably capable of associating the request with

21   the personal data.

22   (ii) It would be unreasonably burdensome for the controller to associate the

23   request with the personal data.

24   (b) For purposes of Subparagraph (a) of this Paragraph, the controller does

25   not do any of the following:

26   (i) Use the personal data to recognize or respond to the consumer who is the

27   subject of the personal data.

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

1   (iii) Sell or otherwise disclose the personal data to any third party other than

2   a processor, except as otherwise permitted in this Chapter.

3   C. A controller who uses deidentified data shall take reasonable steps to

4   ensure the controller does all of the following:

5   (1) Complies with any contractual obligation to which the deidentified data

6   is subject.

7   (2) Promptly addresses any breach of a contractual obligation described in

8   Paragraph (1) of this Subsection.

9   §1391. Limitations

10   A. The requirements described in this Chapter do not restrict a controller's

11 or processor's ability to do any of the following:

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

13   (2) Comply with a civil, criminal, or regulatory inquiry, investigation,

14 subpoena, or summons by a federal, state, local, or other governmental entity.

15   (3) Cooperate with a law enforcement agency concerning activity that the

16 controller or processor reasonably and in good faith believes may violate federal,

17 state, or local laws, rules, or regulations.

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

19   (5) Provide a product or service requested by a consumer or a parent or legal

20 guardian of a child.

21   (6) Perform a contract to which the consumer or the parent or legal guardian

22 of a child is a party, including fulfilling the terms of a written warranty or taking

23 steps at the request of the consumer or parent or legal guardian prior to entering into

24 the contract with the consumer.

25   (7) Take immediate steps to protect an interest that is essential for the life or

26 physical safety of the consumer or of another individual.

27   (8)(a) Detect, prevent, protect against, or respond to a security incident,

28 identity theft, fraud, harassment, malicious or deceptive activity, or any illegal

29 activity.

1   (b)   Investigate, report, or prosecute a person responsible for an action

2   described in Subparagraph (a) of this Paragraph.

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

4   (b)   Investigate, report, or prosecute a person responsible for harming or

5   threatening the integrity or security of systems, as applicable.

6   (10) If the controller discloses the processing in a notice described in R.S.

7   51:1389, engage in public or peer-reviewed scientific, historical, or statistical

8   research in the public interest that adheres to all other applicable ethics and privacy

9   laws.

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

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

12   (a)   Conduct internal analytics or other research to develop, improve, or

13   repair a controller's or processor's product, service, or technology.

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

15   functionality.

16   (c) Effectuate a product recall.

17   (13) Process personal data to perform an internal operation that is either of

18   the following:

19   (a)   Reasonably aligned with the consumer's expectations based on the

20   consumer's existing relationship with the controller.

21   (b) Otherwise compatible with processing to aid the controller or processor

22   in providing a product or service specifically requested by a consumer or a parent or

23   legal guardian of a child or the performance of a contract to which the consumer or

24   a parent or legal guardian of a child is a party.

25   (14)   Retain a consumer's email address to comply with the consumer's

26   request to exercise a right.

27   B. This Chapter does not apply if a controller's or processor's compliance

28   with this Chapter does any of the following:

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

1	(2) As part of a privileged communication, prevents a controller or processor

2	from providing personal data concerning a consumer to a person covered by an

3	evidentiary privilege provided in the laws of this state.

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

5	C. A controller or processor is not in violation of this Chapter if all of the

6	following are true:

7	(1) The controller or processor discloses personal data to a third-party

8	controller or processor in compliance with this Chapter.

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

10	(3) The disclosing controller or processor did not have actual knowledge of

11	the third party's intent to commit a violation of this Chapter.

12	D. If a controller processes personal data in accordance with an exemption

13	described in Subsection C of this Section, the controller bears the burden of

14	demonstrating that the processing qualifies for the exemption.

15	E. Nothing in this Chapter requires a controller, processor, third party, or

16	consumer to disclose a trade secret.

17	§1392. No private cause of action

18	A violation of this Chapter does not provide a basis for, nor is a violation of

19	this Chapter subject to, a private right of action pursuant to this Chapter or any other

20	law.

21	§1393. Investigative powers

22	A. The division shall establish and administer a system to receive consumer

23	complaints regarding a controller's or processor's alleged violation of this Chapter.

24	B.(1) The division may investigate a consumer complaint to determine

25	whether the controller or processor violated or is violating this Chapter.

26	(2) If the director has reasonable cause to believe that substantial evidence

27	exists that a person identified in a consumer complaint is in violation of this Chapter,

28	the director shall refer the matter to the attorney general.

1   (3) Upon request, the division shall provide consultation and assistance to

2   the attorney general in enforcing this Chapter.

3   §1394. Enforcement powers of the attorney general

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

5   B. Upon referral from the division, the attorney general may initiate an

6   enforcement action against a controller or processor for a violation of this Chapter.

7   C.(1) At least thirty days before the day on which the attorney general

8   initiates an enforcement action against a controller or processor, the attorney general

9   shall provide the controller or processor with all of the following:

10   (a) Written notice identifying each provision of this Chapter the attorney

11   general alleges the controller or processor has violated or is violating.

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

13   (2) The attorney general may not initiate an action if the controller or

14   processor does all of the following:

15   (a) Cures the noticed violation within thirty days after the day on which the

16   controller or processor receives the written notice described in Paragraph (1) of this

17   Subsection.

18   (b) Provides the attorney general an express written statement that attests to

19   both of the following:

20   (i) The violation has been cured.

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

22   (3) The attorney general may initiate an action against a controller or

23   processor who does either of the following:

24   (a) Fails to cure a violation after receiving the notice described in Paragraph

25   (1) of this Subsection.

26   (b) After curing a noticed violation and providing a written statement in

27   accordance with Paragraph (2) of this Subsection, continues to violate this Chapter.

28   (4) In an action described in this Section, the attorney general may recover

29   all of the following:

1   (a) Actual damages to the consumer.

2   (b) For each violation described in Paragraph (3) of this Subsection, a civil

3 fine in an amount not to exceed seven thousand five hundred dollars.

4   D. All money received from an action pursuant to this Chapter shall be

5 deposited into the Consumer Privacy Account established in R.S. 51:1395.

6   E. If more than one controller or processor are involved in the same

7 processing in violation of this Chapter, the liability for the violation shall be

8 allocated among the controllers or processors according to the principles of

9 comparative fault.

10 §1395. Data protection assessments

11   A. A controller shall not conduct processing that presents a heightened risk

12 of harm to a consumer without conducting and documenting a data protection

13 assessment of each of its processing activities that involve personal data acquired on

14 or after the effective date of this Chapter that present a heightened risk of harm to a

15 consumer.

16   B. For purposes of this Section, "processing that presents a heightened risk

17 of harm to a consumer" includes all of the following:

18   (1) Processing personal data for purposes of targeted advertising or for

19 profiling if the profiling presents a reasonably foreseeable risk of any of the

20 following:

21   (a) Unfair or deceptive treatment of consumers.

22   (b) Unlawful disparate impact on consumers.

23   (c) Financial or physical injury to consumers.

24   (d) An intrusion, physical or otherwise, upon the solitude or seclusion, or the

25 private affairs or concerns of consumers, if the intrusion would be offensive to a

26 reasonable person.

27   (e) Other substantial injury to consumers.

28   (2) Selling personal data.

29   (3) Processing sensitive data.

1   C. Data protection assessments shall identify and weigh the benefits that may

2   flow, directly and indirectly, from the processing to the controller, the consumer,

3   other stakeholders, and the public against the potential risks to the rights of the

4   consumer associated with the processing, as mitigated by safeguards that the

5   controller can employ to reduce the risks. The controller shall factor into this

6   assessment the use of deidentified data and the reasonable expectations of

7   consumers, as well as the context of the processing and the relationship between the

8   controller and the consumer whose personal data will be processed.

9   D. A controller shall make the data protection assessment available to the

10   attorney general upon request. The attorney general may evaluate the data protection

11   assessment for compliance with the duties provided for in this Chapter. Data

12   protection assessments are confidential and exempt from public inspection and

13   copying in accordance with the Public Records Law as provided in R.S. 44:1 et seq.

14   The disclosure of a data protection assessment pursuant to a request from the

15   attorney general pursuant to this Subsection does not constitute a waiver of any

16   attorney-client privilege or work-product protection that might otherwise exist with

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

18   E. A single data protection assessment may address a comparable set of

19   processing operations that include similar activities.

20   F. Data protection assessment requirements apply to processing activities

21   created or generated after December 1, 2024.

22   §1396. Consumer privacy restricted account

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

24   Account".

25   B. The account shall be funded by money received through civil enforcement

26   actions pursuant to this Chapter.

27   C. Upon appropriation, the division or the attorney general may use money

28   deposited into the account for any of the following:

1   (1) Investigative and administrative costs incurred by the division in

2   investigating consumer complaints alleging violations of this Chapter.

3   (2) Recovery of costs and attorney fees accrued by the attorney general in

4   enforcing this Chapter.

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

6   following:

7   (a) Consumer rights pursuant to this Chapter.

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

9   processors.

10   D. If the balance in the account exceeds four million dollars at the close of

11   any fiscal year, the state treasurer shall transfer the amount that exceeds four million

12   dollars into the state general fund.

13   §1397. Attorney general report

14   A. The attorney general and the division shall compile a report composed of

15   all of the following:

16   (1) An evaluation of the liability and enforcement provisions of this Chapter,

17   including the effectiveness of the attorney general's and the division's efforts to

18   enforce this Chapter.

19   (2) A summary of the data protected and not protected by this Chapter

20   including, with reasonable detail, a list of the types of information that are publicly

21   available from local, state, and federal government sources.

22   B. The attorney general and the division may update the report as new

23   information becomes available.

24   C. The attorney general and the division shall submit the report to the House

25   Committee on Commerce and Senate Committee on Commerce, Consumer

26   Protection, and International Affairs before July 1, 2026.

27   Section 3. This Act shall become effective on December 31, 2024.

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 947 Original   2024 Regular Session   Davis

Abstract: Provides relative to the protection of data by certain persons and entities.

Proposed law shall be known and may be cited as "The Louisiana Consumer Privacy Act".

Proposed law provides for definitions.

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 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 a 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.

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

Proposed law preempts any conflicting local regulation.

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 or accurate summary of his personal data.

(4)   Correct inaccuracies in the personal data.

(5)   Delete the personal data that was supplied by the consumer.

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

Proposed law provides that 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.

Proposed law provides that a controller who charges a fee based on the exceptions in proposed law bears the burden of proving that the necessary criteria are met.

Proposed law allows a controller to request additional information from a consumer if reasonably necessary to respond to the request.

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

Proposed law requires that prior to performing on behalf of a controller, the processor and controller 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 provides for the determination of a person as a controller or processor.

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 a 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.

Proposed law does not require a controller to provide a product, service, or functionality to a consumer in certain circumstances.

Proposed law cannot be waived or limited through a contractual provision.

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 he complies with all contractual obligations relative to that data and to promptly address any breach of the contract.

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 another.

Proposed law provides that a controller or processor is not in violation of proposed law if he provides data to a third party in accordance with proposed law and the third party then processes the data in violation of proposed law, if he had no knowledge of the intent to commit a violation. If a controller or processor processes data pursuant to an exception in proposed law, he bears the burden of proving that the necessary criteria are met.

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.

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

Proposed law provides that a violation of proposed law does not provide a basis for a private cause of action.

Proposed law requires that a system to receive consumer complaints be established and administered by the consumer protection section within the Dept. of Justice.

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

Proposed law allows the attorney general to initiate an action if the controller continues to violate proposed law after remedying the problem and providing notice. The attorney general may recover actual damages to the consumer and a civil fine of up to $7,500 per violation of proposed law.

Proposed law provides that if a controller and processor are involved in the same violation of proposed law, comparative fault is used to allocate liability.

Proposed law creates the Consumer Privacy Account (account) where all monies received from an action arising out of proposed law are to be deposited. Further provides that the money in the account may be used for investigative and administrative costs, recovery of costs and attorney 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, 2026.

Effective December 31, 2024.

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