SUBJECT: Regulating the collection and processing of certain personal data

COMMITTEE: Business & Industry — committee substitute recommended

VOTE: 8 ayes — Longoria, Vasut, Cole, Frazier, J. González, Hinojosa, Isaac, Lambert

0 nays

1 absent — Neave Criado

WITNESSES: For — Stephen Scurlock, Independent Bankers Association of Texas; Ryan Harkins, Microsoft; Servando Esparza, TechNet; Briana Gordley, Texas Appleseed; Megan Mauro, Texas Association of Business; David Dunmoyer, Texas Public Policy Foundation (*Registered, but did not testify*: Travis Krogman, Austin Chamber of Commerce; Melodie Durst, Credit Union Coalition of Texas; Annie Spilman, NFIB; David Foy, RELX Inc.; Celeste Embrey, Texas Bankers Association; Jennifer Mudge, Texas Council on Family Violence; Larry Gonzales, Texas Credit Union Association; Danielle Lobsinger Bush, Texas Healthcare and Bioscience Institute; Caleb Troxclair, Texas.net; Aaron Day, TLTA; Fred Shannon, WalMart; Thomas Parkinson)

Against — Steve Perkins; Gregory Porter (*Registered, but did not testify*: Susan Stewart)

On — Jordan Crenshaw, US Chamber of Commerce (*Registered, but did not testify*: Laird Doran, Gulf States Toyota; Steven Robinson, Office of the Texas Attorney General)

DIGEST: CSHB 4 would add certain restrictions to the sale and processing of personal consumer data. The bill would apply to a person that conducts business in the state and engages in the sale and processing of personal data. The bill would not apply to:

- state agencies and political subdivisions;

- financial institutions or data subject to certain financial regulations;
- non-profits; or
- institutions of higher education.

CSHB 4 would only apply to small businesses, as defined by the United States Small Business Administration, in circumstances where a small business was selling sensitive personal data and would need the consumer's consent before selling.

Controller duties. A controller would be defined as an individual who alone or jointly with others determined the purpose and means of processing data. CSHB 4 would limit the collection of personal data by a controller to what was adequate, relevant, and necessary for the purpose for which the data was collected, as disclosed to the consumer. The controller could not process personal data for a purpose that was neither reasonable nor compatible with the disclosed purpose without the consumer's consent. The controller also would be required to implement appropriate security practices to protect consumers personal data.

If the controller sold personal data to third parties or processed personal data for targeted advertising, the controller would be required to clearly disclose the process and how a consumer could opt out. CSHB 4 would prohibit controllers from processing sensitive data without a consumer's expressed consent or a parent's consent if the personal information belonged to a child under the age of 13. The controller also could not discriminate against a consumer should they exercise their consumer rights with certain exceptions.

Controllers would be required to post accessible and clear privacy notices that included:

- categories of personal data processed by the controller;
- the purpose for processing personal data;
- how consumer’s could exercise their consumer's rights; and
- categories of personal data shared with third parties, if applicable.

If the controller sold sensitive or biometric data, the controller would be required to post a specific notice that the consumer's data could be sold.

Consumer requests and controllers' duties would not apply to pseudonymous data (information that can not be attributed to a specific individual without the use of additional information) if the controller could prove that any information necessary to identify the consumer was kept separately.

A processor, defined as a person that processes data on behalf of the controller, would be required to adhere to instructions given by the controller and assist the controller in complying with the bill. A processor could arrange for a qualified and independent assessor to examine the processor's policies and organizational measures to ensure they met the requirements of the bill. The processor would be required to provide a report of the assessment to the controller upon request.

Data protection assessment. The controller would be required to conduct a data protection assessment of each of the following processing activities:

- the processing of personal data for targeted advertising;
- the sale of personal data;
- the processing of personal data for profiling that presented certain foreseeable risks;
- the processing of sensitive data; and
- activities that presented heightened risk of harm to consumers.

The data protection assessment would be required to weigh the benefits of the processing activity against the potential risks to the rights of the consumer, including any safeguards that could mitigate risk. The assessment would also be required to factor in the use of deidentified data, (data that can not be reasonably linked to an identified individual or the individual's device), expectations of consumers, the context of the processing activity, and the relationship between the consumer and the controller.

The controller would be required to make a data protection assessment available to the attorney general if requested as part of an investigation. The assessment would remain confidential and exempt from public inspection and copying.

Deidentified or pseudonymous data. A controller with deidentified data would be required to take reasonable measures to ensure that the data could not be attributed to an individual, publicly commit to maintaining and using the data without trying to re-identify the it, and contractually obligate any recipient of deidentified data to comply with provisions of the bill.

Consumer rights. CSHB 4 would give consumers the right to request certain information of the controller. The controller could not waive these rights through any contract or agreement. The controller would be required to comply with an authenticated consumer request to:

- confirm whether the controller was processing the consumer's personal data and to access the data;
- correct inaccuracies in the consumer's personal data;
- delete personal data; or to obtain a copy of the data under certain conditions; or
- opt out of the processing of their data for certain purposes.

CSHB 4 would require the controller to respond to the consumer request no later than 45 days after the request was made. The controller could extend the response period by an additional 45 days if reasonably necessary. The controller would be required to respond to a request from a consumer free of charge at least twice a year unless the consumer request was proven to be excessive, in which case the controller could charge an administrative fee or decline the request.

If the controller denied a request, the controller would be required to inform the consumer why the request was denied and how to appeal. The bill would require the appeal process to be similar to the original process for initiating action by the consumer and the controller would be required

to inform the consumer of any action taken during the appeals process. Should the appeal be denied, the controller would be required to provide an online mechanism through which the consumer could file a complaint with the attorney general.

The controller would be required to establish two or more ways for consumers to submit requests, taking into account how the consumer interacted with the controller, the necessity for secure and reliable communications, and the ability of the controller to authenticate the identity of the consumer. If the controller operated a website, the website would be required to contain a mechanism to submit requests.

Investigative authority. The attorney general would have exclusive authority over enforcement of the bill's provisions and would be required to post on the attorney general's website the responsibilities of controllers and processors as well as consumer's rights and a way for consumers to submit complaints. If the attorney general believes that a person had engaged, was engaged in or was about to engage in a violation of the bill, the attorney general could issue a civil investigative demand. The attorney general could request that the controller disclose a data protection assessment that was relevant to an investigation and evaluate the assessment for compliance.

Before enacting a civil penalty the attorney general would be required to notify the individual no later than 30 days before bringing action and identifying the specific violation. The person would have 30 days to remedy the violation and would be required within the 30 day period to provide a written statement to the attorney general stating that the person had remedied the violation, notified the consumer that the violation was addressed, and provide documentation as to how the violation was remedied as well as internal changes made to prevent future violations.

If a person committed a violation following the remedy period or breached a written statement provided to the attorney general, the person would be liable for a civil penalty of up to $7,500 per violation. The attorney general could bring an action to recover a civil penalty, restrain the person

from violating the chapter, or seek injunctive relief. The attorney general could recover attorney's fees and expenses incurred and would be required to deposit the civil penalty into the state treasury.

If a controller disclosed data to a third party and the third party violated the provisions of the bill, the controller would not be in violation. The third party would also not be in violation of the bill if the third party received personal data from the controller and the controller violated the provisions of the bill.

Data exceptions. The bill would exempt certain data, including:

- protected health information;
- health records;
- data collected from human subjects as part of clinical research;
- other health care related information;
- data processed for the purpose of a job application;
- data processed or maintained as part of an emergency contact; and
- data currently already regulated by federal statute such as the Driver's Privacy Protection Act.

Implementation. The Department of Information Resources (DIR) would be responsible for the review and implementation of the bill. No later than September 1, 2024 the DIR would be required to create an online portal publicly available on its website for the public to provide feedback. DIR would be required publish a public report on the implementation of the bill by January 1, 2025.

This bill would take effect on March 1, 2024

SUPPORTERS SAY:

CSHB 4 would create stronger data privacy regulations by giving consumers the rights and protections they need to keep their data secure. Currently, a lack of regulation of the selling and collection of personal data allows bad actors to obtain data for criminal purposes while also allowing companies to use targeted advertising and profiling at consumers' expense. The bill would give consumers the right to reclaim

their personal data by regulating the data controllers can process. The bill also would help to protect sensitive data, ensuring that data that makes consumers most vulnerable could not be sold or processed without consumers' consent.

CSHB 4 would implement strong enforcement mechanisms through the attorney general's office to hold companies who violate consumer rights accountable and make the process more transparent. Consumers could file complaints through the attorney general's website, ensuring Texans' complaints and voices were heard throughout the process.

The bill also would keep compliance costs low by streamlining the process through which complaints were filed. Additionally, small businesses would be exempt from many of the bill's provisions, allowing them to continue to connect with their customers without being burdened by compliance costs.

CRITICS SAY:

CSHB 4 should mirror data privacy legislation from other states to limit companies' need to navigate different state laws and keep compliance costs to a minimum.

OTHER CRITICS SAY:

The bill should do more to protect Texans' data from being collected and sold. Giving a controller up to 90 days to respond to a consumer request could allow the data to exchanged hands many times, which could make it inaccessible to consumers.

Additionally, under the bill, consumers would be required to submit a request to every website that used their data, which could make regaining control of one's personal information more difficult. The bill should include a universal opt-out provision allowing consumers to opt out of the processing, collection, and sale of the consumer's data across sites.

NOTES:

According to the Legislative Budget Board, the bill would have a negative impact of $7.5 million through the biennium ending August 31, 2025.