BILL ANALYSIS

C.S.H.B. 4
By: Capriglione
Business & Industry
Committee Report (Substituted)

BACKGROUND AND PURPOSE

In the absence of robust federal regulations regarding the collection and use of consumer data, a movement has begun at the state level with various state legislatures looking to set their own standards. The State of Texas has not yet established comprehensive regulations for the collection, use, processing, and treatment of consumers' personal data by certain business entities. C.S.H.B. 4 seeks to do so by enacting the Texas Data Privacy and Security Act, which aims to maximize both the utility of the rights provided to consumers and interoperability with other states to minimize compliance costs for businesses.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B. 4 amends the Business & Commerce Code to enact the Texas Data Privacy and Security Act, which regulates the collection, use, processing, and treatment of consumers' personal data by certain business entities. For purposes of this act, a "consumer" is an individual who is a Texas resident acting only in an individual or household context, and the term does not include an individual acting in a commercial or employment context. "Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual and does not include deidentified data or publicly available information, but the term does include pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. An "identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.

The regulations established by the act apply only to a person processing or engaging in the sale of personal data who conducts business in Texas or produces a product or service consumed by Texas residents and apply only if the person is not a small business as defined by the U.S. Small Business Administration (SBA), with the exception of a requirement expressly applicable to small businesses regarding consumer consent. The regulations do not apply to the processing of personal data by a person in the course of a purely personal or household activity or to any of the following:

- an executive branch state agency or a political subdivision;
- a financial institution or data subject to the federal Gramm-Leach-Bliley Act's privacy protections;

- a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the federal Health Information Technology for Economic and Clinical Health Act;
- a public, private, or independent institution of higher education; or
- any of the following nonprofit organizations:
    - a corporation organized under the Business Organizations Code, to the extent applicable to nonprofit corporations;
    - a 501(c)(3), 501(c)(6), or 501(c)(12) tax-exempt organization;
    - a 501(c)(4) tax-exempt organization primarily dedicated to the detection, investigation, and prosecution of insurance fraud;
    - a political organization; or
    - a subsidiary or affiliate of an electric utility regulated under the Public Utility Regulatory Act.

Consumer Rights

C.S.H.B. 4 establishes a set of rights for consumers with respect to their personal data. The bill entitles a consumer to exercise these rights at any time by submitting a request to a controller, which is an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data. The request must specify the applicable 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 the child's behalf. The bill requires a controller to comply with an authenticated consumer request to exercise one of the established rights unless an exception is provided by the act, with an authenticated request being one that has been verified through reasonable means to have come from the same consumer whose personal data is at issue.

List of Rights

C.S.H.B. 4 establishes the right of a consumer to do the following:

- confirm whether a controller is processing the consumer's personal data and to access the personal data;
- correct inaccuracies in the consumer's personal data, taking into account the nature of the data and the purposes of the processing of the data;
- delete personal data provided by or obtained about the consumer;
- 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; or
- opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision made by the controller concerning the consumer that results in the provision or denial by the controller of the following:
    - financial and lending services;
    - housing, insurance, or health care services;
    - education enrollment;
    - employment opportunities;
    - criminal justice; or
    - access to basic necessities, such as food and water.

Methods for Submitting Requests

C.S.H.B. 4 requires a controller to establish two or more secure and reliable methods to enable consumers to submit a request to exercise their consumer rights and sets out certain factors those

methods must take into account. A controller may not require a consumer to create a new account to exercise their rights but may require a consumer to use an existing account.

C.S.H.B. 4 requires a controller that maintains a website to provide a mechanism on the website for consumers to submit requests for information required to be disclosed under the act. However, 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 for such information.

Controller Response to Consumer Request

C.S.H.B. 4 requires a controller to respond to a consumer request without undue delay, which may not be later than the 45th day after the date of receipt of the request, except that the controller may extend the response period once by an additional 45 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 and the reason for the extension within the initial 45-day response period. If declining to take action regarding the request, the controller must inform the consumer without undue delay, which may not be later than the 45th day after the date of receipt of the request, of the justification for declining to take action and must also provide instructions on how to appeal the decision.

C.S.H.B. 4 requires a controller to provide information in response to a request free of charge, at least twice annually per consumer, except that if a request is manifestly unfounded, excessive, or repetitive the controller may charge a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request altogether. The controller bears the burden of demonstrating that the request is manifestly unfounded, excessive, or repetitive.

C.S.H.B. 4 establishes that a controller that is unable to authenticate a consumer's request using commercially reasonable efforts is not required to comply with the request and authorizes the controller to request that the consumer provide additional information necessary to authenticate the consumer and their request. The bill further establishes that 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 by taking either of the following actions:

- 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; or
- opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt from the act's regulations.

Appeal

C.S.H.B. 4 requires a controller to 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 decision. The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request. The bill requires a controller to inform the consumer in writing of any action taken or not taken in response to an appeal not later than the 60th day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision, and requires a controller that denies an appeal to provide the consumer with the online mechanism required by the act through which the consumer may contact the attorney general to submit a complaint.

Prohibited Waiver or Limitation of Consumer Rights

C.S.H.B. 4 renders any provision of a contract or agreement that waives or limits in any way a consumer right established by the act void and unenforceable as contrary to public policy.

Controller and Processor Data-Related Duties and Prohibitions

Controller Duties; Transparency

C.S.H.B. 4 requires a controller to limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that data is processed, as disclosed to the consumer. The bill requires a controller, for purposes of protecting the confidentiality, integrity, and accessibility of personal data, to 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. The bill prohibits a controller from doing any of the following:

- processing personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the data is processed, as disclosed to the consumer, without the consumer's consent, except as otherwise provided by the act;
- processing personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;
- discriminating against a consumer for exercising any of the consumer rights contained in this act, 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; or
- processing a consumer's sensitive data without obtaining the consumer's consent, or, in processing the sensitive data of a known child, without complying with the federal Children's Online Privacy Protection Act.

The prohibition against discrimination based on a consumer's exercise of their consumer rights expressly 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 their right to opt out of the processing of their personal data for purposes of targeted advertising, data sales, or profiling or if the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Privacy Notice

C.S.H.B. 4 requires a controller to provide consumers with a reasonably accessible and clear privacy notice regarding the processing and sharing of personal data and how a consumer may exercise their consumer rights. The bill sets out the required contents of such a notice and requires a controller that engages in the sale of personal data that is sensitive data or biometric data to include an additional notice posted in the same location and manner as the general privacy notice informing consumers that the website may sell the applicable data.

Sale of Data to Third Parties and Processing of Data for Targeted Advertising

C.S.H.B. 4 requires a controller that sells personal data to third parties or processes personal data for targeted advertising to clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process. The bill defines "targeted advertising" as displaying to a consumer an advertisement that is selected based on personal data obtained 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:

- the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency; and
- an advertisement that is directed to a consumer in response to the consumer's request for information or feedback or is based on:
    - activities within the controller's own websites or online applications; or
    - the context of a consumer's current search query, visit to a website, or online application.

Duties of Processors

C.S.H.B. 4 requires a person processing personal data on a controller's behalf to adhere to the controller's instructions and assist the controller in meeting or complying with the controller's duties or requirements under the act. The bill sets out certain specific forms of assistance a processor must provide to a controller and provides for a contract between a controller and processor that governs the processor's data processing procedures. The bill authorizes a processor to 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 act using an appropriate and accepted control standard or framework and assessment procedure. The bill requires the processor to provide a report of the assessment to the controller on request.

C.S.H.B. 4 prohibits these provisions relating to processor duties from being 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 the act. The bill establishes that 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 and further establishes that 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.

Data Protection Assessments

C.S.H.B. 4 requires a controller to conduct and document a data protection assessment of each of the following processing activities involving personal data:

- the processing of personal data for purposes of targeted advertising;
- the sale of personal data;
- the processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:
    - unfair or deceptive treatment of or unlawful disparate impact on consumers;
    - financial, physical, or reputational injury to consumers;
    - 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; or
    - other substantial injury to consumers;
- the processing of sensitive data; and
- any processing activities involving personal data that present a heightened risk of harm to consumers.

The bill requires the assessment to 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 risk reduction safeguards that can be employed. The bill sets out certain factors that the assessment must address and authorizes a single assessment to address a comparable set of processing operations that include similar activities. These data protection assessments apply only to processing activities generated after the bill's effective date and are not retroactive.

C.S.H.B. 4 requires the controller to make an assessment available to the attorney general on request pursuant to a civil investigative demand. The bill makes an assessment confidential and exempt from public inspection and copying under state public information law and establishes that disclosure of the 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. The bill establishes that a data protection assessment conducted by a controller for the purpose of compliance with other laws

or regulations may constitute compliance with the act's requirements if the assessment has a reasonably comparable scope and effect.

Deidentified or Pseudonymous Data

C.S.H.B. 4 sets out provisions applicable to deidentified data and pseudonymous data, which are defined as follows:

- "deidentified data" is data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to that individual; and
- "pseudonymous data" is 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 data is not attributed to an identified or identifiable individual.

C.S.H.B. 4 requires a controller in possession of deidentified data to do the following:

- take reasonable measures to ensure that the data cannot be associated with an individual;
- publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and
- contractually obligate any recipient of the deidentified data to comply with the act.

C.S.H.B. 4 prohibits its provisions from being construed to require a controller or processor to do any of the following:

- reidentify deidentified data or pseudonymous data;
- 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; or
- comply with an authenticated consumer rights request, if the controller:
    - is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to do so;
    - does not use the personal data to recognize or respond to the specific consumer who is the subject of the data or associate the data with other personal data about the same specific consumer; and
    - does not sell the personal data to any third party or otherwise voluntarily disclose the data to any third party other than a processor, except as otherwise permitted.

C.S.H.B. 4 makes the list of specific controller duties regarding transparency and the consumer rights to confirm the processing of their personal data, access their personal data, correct data inaccuracies, delete personal data, and obtain a copy of their personal data inapplicable 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. The bill requires a controller that discloses pseudonymous or deidentified data to exercise reasonable oversight to monitor compliance with any contractual commitments to which the data is subject and take appropriate steps to address any breach of those contractual commitments.

Requirements for Small Businesses

C.S.H.B. 4 requires a person who is a small business as defined by the SBA to receive prior consent from the consumer before engaging in the sale of personal data that is sensitive data. The bill clarifies that a person who violates this requirement is subject to the civil penalty created by the bill.

Enforcement

Enforcement and Investigative Authority

C.S.H.B. 4 grants exclusive authority to enforce the act to the attorney general. The bill authorizes the attorney general to issue a civil investigative demand if the attorney general has reasonable cause to believe that a person has engaged in, is engaging in, or is about to engage in a violation of the act. The procedures established for the issuance of a civil investigative demand under the Texas Free Enterprise and Antitrust Act of 1983 apply to the same extent and manner to the issuance of a civil investigative demand by the attorney general using this investigative authority.

C.S.H.B. 4 authorizes the attorney general to request, pursuant to such an issued civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The attorney general may evaluate the data protection assessment for compliance with the requirements set forth for controllers under the act regarding transparency, privacy notices for consumers, and disclosure with respect to data sold to a third party or processed for targeted advertising.

Civil Penalty; Injunction; Opportunity to Cure

C.S.H.B. 4 establishes procedures that give a person a 30-day period in which to cure an identified violation of the act and prohibits the attorney general from bringing an action if the person cures the violation within that period and provides the attorney general a written statement that the person did the following:

- cured the alleged violation;
- notified the consumer that the consumer's privacy violation was addressed;
- provided supportive documentation to show how the privacy violation was cured; and
- made changes to internal policies to ensure that no further violations will occur.

The bill makes a person who is still in violation following the prescribed cure period or who breaches the written statement provided to the attorney general liable for a civil penalty capped at $7,500 for each violation. The bill authorizes the attorney general to bring an action in the name of the state to recover the civil penalty, restrain or enjoin the person from continued violations, or recover the civil penalty and seek injunctive relief. The attorney general may recover reasonable attorney's fees and other reasonable expenses incurred in investigating and bringing the action and requires the attorney general to deposit the civil penalty in the state treasury to the credit of the general revenue fund.

Website and Complaint Mechanism

C.S.H.B. 4 requires the attorney general to post the following on the attorney general's website not later than March 1, 2024:

- information relating to the responsibilities of a controller and a processor under the act and the consumer personal data rights established by the act; and
- an online mechanism through which a consumer may submit a complaint under the act to the attorney general.

No Private Right of Action

C.S.H.B. 4 expressly may not be construed as providing a basis for, or being subject to, a private right of action for a violation of its provisions or any other state law.

Protections for Disclosure of Personal Data to Third-Party Controller of Processor

C.S.H.B. 4 establishes that a controller or processor that discloses personal data to a third-party controller or processor that is in violation of the act is not also themselves in violation if the

disclosure was done in compliance with the act and, at the time of the disclosure, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. Moreover, the bill establishes that a third-party controller or processor receiving personal data from a controller or processor that is in compliance with the act is not considered in violation of the act for the transgressions of the controller or processor from which the third-party controller or processor receives the personal data.

Construction of the Texas Data Privacy and Security Act

C.S.H.B. 4 prohibits its provisions from being construed to do any of the following:

- restrict a controller's or processor's ability to do, or assist another controller, processor, or third party in doing, the following:
    - comply with applicable laws, rules, or regulations or a governmental inquiry, investigation, subpoena, or summons;
    - investigate, establish, exercise, prepare for, or defend legal claims;
    - provide a product or service that is specifically requested by a consumer or, if applicable, their parent or guardian;
    - perform a contract to which a consumer is a party;
    - take steps at the request of a consumer before entering into a contract;
    - take immediate steps to protect an interest that is essential for life or physical safety and in which the processing cannot be manifestly based on another legal basis;
    - prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
    - preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security; and
    - engage in public or peer-reviewed scientific or statistical research that is in the public interest, subject to certain conditions;
- prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under state law as part of a privileged communication;
- impose a requirement on controllers and processors that adversely affects the rights or freedoms of any person, including the right of free speech; or
- require a controller, processor, third party, or consumer to disclose a trade secret.

The processing of personal data by an entity for any of these purposes does not solely make the entity a controller with respect to the processing of the data.

Exempted Purposes

C.S.H.B. 4 makes a requirement imposed on a controller or processor under the act inapplicable if compliance would violate an evidentiary privilege under state law. The bill prohibits the requirements imposed on controllers and processors from restricting a controller's or processor's ability to collect, use, or retain data for any of the following purposes:

- conducting internal research to develop, improve, or repair products, services, or technology;
- effecting a product recall;
- identifying and repairing technical errors that impair existing or intended functionality; or
- performing certain internal operations.

The bill sets out certain requirements for personal data collected, used, or retained for such an exempted purpose relating to accounting for the data's nature and purpose; protecting confidentiality, integrity, and accessibility; and reducing risks of harm to consumers. The bill also establishes certain limitations on the processing of personal data for any of these exempted purposes or an exempted purpose outlined in the provisions relating to the act's construction. A controller that processes personal data for an exempted purpose bears the burden of

demonstrating that the processing qualifies for the exemption and complies with these requirements and limitations.

Local Preemption

C.S.H.B. 4 supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or processor.

Exempt Information

C.S.H.B. 4 exempts from its provisions the following information:

- health information protected under HIPAA;
- health records, which means any written, printed, or electronically recorded material maintained by a health care provider, as defined under HIPAA, in the course of providing health care services to an individual that concerns the individual and the services provided, including the substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services or information otherwise acquired by the provider about an individual in confidence and in connection with the provision of such services;
- information considered patient identifying information for purposes of certain federal confidentiality protections relating to substance abuse and mental health;
- identifiable private information:
    - for purposes of the federal policy for the protection of human subjects;
    - 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 (ICH) or of the protection of human subjects under applicable federal regulations; or
    - that is personal data used or shared in research conducted in accordance with the act or other research conducted in accordance with applicable law;
- information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986;
- information considered patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act of 2005;
- information derived from any of the health care-related information included in this list of exemptions that is deidentified in accordance with HIPAA;
- information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information included in this list of exemptions that is maintained by a covered entity or business associate as defined by HIPAA or by a program or a qualified service organization as defined for purposes of certain federal confidentiality protections relating to substance abuse and mental health;
- information included in a limited data set authorized to be disclosed under HIPAA, to the extent that the information is used, disclosed, and maintained in the manner provided by HIPAA;
- information collected or used only for public health activities and purposes as authorized by HIPAA;
- 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 federal Fair Credit Reporting Act;
- personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;
- personal data regulated by the federal Family Educational Rights and Privacy Act of 1974;

- personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act of 1971;
- 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;
- data processed or maintained as the emergency contact information of an individual that is used for emergency contact purposes; and
- data that is processed or maintained and is necessary to retain to administer benefits for another individual that relates to an individual who is applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party and used for the purposes of administering those benefits.

Parental Consent

C.S.H.B. 4 establishes that a controller or processor that complies with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act with respect to data collected online is considered to be in compliance with any requirement of the act to obtain parental consent.

Definitions

C.S.H.B. 4 defines the following terms, among others:

- "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, and for such purposes "control" or "controlled" means the following:
    - the ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;
    - the control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or
    - the power to exercise controlling influence over the management of a company;
- "biometric data" means data generated by automatic measurements of an individual's biological characteristics and does not include a physical or digital photograph, a video or audio recording or data generated from such a recording, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA;
- "child" means an individual younger than 13 years of age and "known child" means a child under circumstances where a controller has actual knowledge of, or wilfully disregards, the child's age;
- "consent," when referring to a consumer, means a clear affirmative act, written statement, electronic statement, or other unambiguous affirmative action signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer but does not include acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other unrelated information, hovering over, muting, pausing or closing a given piece of content, or agreement obtained through the use of dark patterns;
- "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 such;
- "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 the following:
    - 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; or
    - the election of a presidential/vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed;

- "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;
- "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;
- "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;
- "sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party and specifically excludes the following:
    - disclosure of personal data to a processor that processes the data on the controller's behalf;
    - disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
    - disclosure or transfer of personal data to an affiliate of the controller;
    - 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; or
    - disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition;
- "sensitive data" means a category of personal data that includes:
    - personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
    - genetic or biometric data processed for the purpose of uniquely identifying an individual;
    - personal data collected from a known child; and
    - precise geolocation data derived from technology that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet, excluding 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;
- "third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor; and
- "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:
    - the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and
    - 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.

Implementation

C.S.H.B. 4 requires the Department of Information Resources (DIR), under the management of the chief privacy officer, to review the implementation of the act. The bill requires DIR to create,

not later than September 1, 2024, an online portal available on the DIR website for members of the public to provide feedback and recommend changes to the act. The portal must remain open for at least 90 days. The bill requires DIR, not later than January 1, 2025, to make available to the public a report detailing the status of the act's implementation and make any recommendations to the legislature regarding changes to the act. These provisions expire September 1, 2025.

Severability

C.S.H.B. 4 includes a severability clause.

EFFECTIVE DATE

March 1, 2024.

COMPARISON OF INTRODUCED AND SUBSTITUTE

While C.S.H.B. 4 may differ from the introduced in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute includes provisions not in the introduced that do the following:

- require a small business to receive prior consent from the consumer before engaging in the sale of personal data that is sensitive data;
- require the attorney general to post on the attorney general's website not later than March 1, 2024, information relating to the responsibilities of a controller and a processor and the established consumer personal data rights, along with an online mechanism through which a consumer may submit a complaint;
- require a controller who engages in the sale of personal data that is sensitive data or biometric data to include an additional notice indicating that the controller's website may sell the applicable data along with the general privacy notice that a controller must provide to consumers; and
- make the requisite data protection assessments applicable only with respect to processing activities generated after the bill's effective date.

The substitute exempts from the act information included in a limited data set authorized to be disclosed under HIPAA, to the extent that the information is used, disclosed, and maintained in the manner provided by HIPAA, whereas the introduced did not exempt this information.

Whereas the substitute included among the nonprofit organizations exempt from the act a subsidiary or affiliate of an entity organized under the general provisions of the Public Utility Regulatory Act (PURA), the substitute includes among those exempt nonprofit organizations instead a subsidiary or affiliate of an electric utility regulated under PURA.

The substitute revises the definitions of "identified or identifiable individual," "personal data," "pseudonymous data," and "profiling" as follows:

- whereas the introduced defined "identified or identifiable individual" as any individual who can be readily identified, directly or indirectly, the substitute limits this definition only to consumers;
- whereas in the introduced pseudonymous data was classified as "personal data" if it is linked or reasonably linkable to an identified or identifiable individual, the substitute classifies pseudonymous data as personal data only if it is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual;
- whereas the introduced defined the term "pseudonymous data" as personal data that cannot be attributed to a specific individual without the use of additional information,

the substitute broadens the definition of the term to encompass any information, regardless of whether it is classified as personal data, that cannot be attributed to a specific individual without the use of additional information; and

- whereas the introduced defined "profiling" as any form of automated processing performed on personal data to evaluate, analyze, or predict certain personal aspects, the substitute limits the definition to any form of such processing that is solely automated.

Whereas the introduced required a controller to provide information in response to a consumer request free of charge up to twice annually per consumer, the substitute provides that a controller must provide a free response at least twice annually per consumer.

The substitute revises the requirement established in the introduced for a controller to make a data protection assessment available to the attorney general to specify that this requirement applies only when pursuant to a civil investigative demand.

Both the introduced and the substitute prohibit the attorney general from bringing an action against a person for a violation of the act if the person cures the violation within the prescribed period and provides a certain statement to the attorney general. However, whereas the introduced required the statement to indicate only that the alleged violation was cured and no further violations will occur, the substitute requires the statement to indicate that the person did the following:

- cured the violation;
- notified the consumer that the consumer's privacy violation was addressed;
- provided supportive documentation to show how the privacy violation was cured; and
- made changes to internal policies to ensure that no further violations will occur.

Both the introduced and the substitute contain provisions establishing that there is no private right of action. However, whereas the introduced established that the act may not be construed to create a private right of action for a violation of the act or any other chapter, the substitute establishes that the act may not be construed as providing a basis for, or being subject to, a private right of action for the violation of the act or any other law.

The substitute changes the deadline for DIR to create the online portal for public feedback and recommendations from March 1, 2024, as in the introduced, to September 1, 2024.

The substitute changes the bill's effective date from September 1, 2023, as in the introduced, to March 1, 2024.