OLR Bill Analysis

sSB 893

AN ACT CONCERNING CONSUMER PRIVACY.

SUMMARY

This bill establishes a framework for controlling and processing personal data. Among other things, it:

1. establishes responsibilities and privacy protection standards for data controllers (those that determine the purpose and means of processing personal data) and processors (those that process data for a controller);

2. grants consumers the right to access, correct, delete, and obtain a copy of personal data and to opt out of the processing of personal data for certain purposes (e.g., targeted advertising);

3. requires data protection assessments;

4. authorizes the attorney general to bring an action to enforce the bill's requirements; and

5. subjects violators to a $7,500 civil fine per violation.

The bill's consumer data privacy requirements generally apply to individuals (1) conducting business in Connecticut or producing products or services targeted to Connecticut residents and (2) controlling or processing personal data above specified consumer thresholds.

The bill exempts (1) various entities, including state and local governments, certain financial institutions, certain health entities, nonprofits, and higher education institutions and (2) specified information and data, including certain health records, identifiable private information for human research, certain credit-related

information, and certain information collected under specified federal laws.

EFFECTIVE DATE: January 1, 2023

§§ 1 & 2 — CONTROLLERS AND PROCESSORS SUBJECT TO THE BILL'S REQUIREMENTS

The bill's requirements generally apply to individuals and entities that conduct business in Connecticut or produce products or services targeting Connecticut residents and control or process personal data of at least (1) 100,000 consumers during a calendar year, or (2) 25,000 consumers and derive more than 50% of their gross revenue from selling personal data. The bill defines a consumer as a natural person who is a state resident and acting only in an individual or household context; it does not include a natural person acting in a commercial or employment context.

Under the bill, a "controller" is a natural or legal person who, alone or jointly with others, determines the purpose and means of processing personal data. A "processor" is a natural or legal entity that processes personal data on a controller's behalf.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person but does not include de-identified data or publicly available information. "Publicly available information" means information that is lawfully made available through federal, state, or municipal 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 the consumer, or by a person the consumer has disclosed the information to, unless the consumer has restricted the information to a specific audience.

"Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, including collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.

§ 3 — EXEMPTIONS

Entities

The bill does not apply to any:

1. body, authority, board, bureau, commission, district, or agency of the state or its political subdivisions;

2. financial institution or data subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

3. entity (e.g., insurer or health care provider) subject to federal privacy, security, and breach notification rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act;

4. 501(c)(3) nonprofit organization; or

5. private or public higher education institution.

Information and Data

The bill also exempts the following information and data:

1. protected health information under HIPAA (42 U.S.C. 1320d et seq.);

2. health records (e.g., continuity of care documents, discharge summaries, and other patient health information);

3. patient identifying information for purposes of a federal substance abuse and mental health law (42 U.S.C. 290dd-2);

4. identifiable private information for the purposes of the federal policy for protecting human subjects (45 C.F.R. Part 46);

5. identifiable private information that is collected as part of human subject research under the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

6. information and data related to protecting human subjects (21 C.F.R. Parts 6, 50, and 56) or personal data used or shared in research that is conducted in accordance with the standards protecting human subjects the bill exempts above, or other research conducted in accordance with applicable law (45 C.F.R. 164.501);

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

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

9. information derived from any health care related information listed in the information or data exemption list that is de-identified according to HIPAA's de-identification requirements;

10. information originating from, and intermingled to be indistinguishable with, or treated in the same manner as exempt information under the bill, maintained by a covered entity or business associate, program, or qualified service organization, as specified in a federal law related to substance abuse and mental health (42 U.S.C. 290dd-2);

11. information used for public health activities and purposes as authorized by HIPAA;

12. the collection, maintenance, disclosure, sale, communication, or use of any personal information relating to a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that activity is regulated by and authorized under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

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

14. personal data regulated by the Family Educational Rights and Privacy Act (20 U.S.C. 1232g et seq.);

15. personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act (12 U.S.C. 2001 et seq.); and

16. data processed or maintained (a) in the course of an individual applying to, 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; (b) as an individual's emergency contact information and used for emergency contact purposes; or (c) that is necessary to retain to administer benefits for another individual relating to the individualwith health information protected under HIPAA and used for administering the benefits.

Parental Consent Exemption

The bill deems controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.) as compliant with any obligation to obtain parental consent under the bill.

§ 4 — CONSUMER RIGHTS

Under the bill, consumers may invoke the rights the bill authorizes at any time by submitting a request to a controller specifying the right they want to invoke. A known child's parent or legal guardian may invoke the consumer rights on the child's behalf regarding processing the child's personal data. The bill defines a "child" as someone under age 13.

The bill allows consumers to exercise the following rights:

1. confirm whether or not a controller is processing the consumer's personal data and access the data;

2. correct inaccuracies in the consumer's personal data, considering the nature of the personal data and the purposes of processing the data;

3. delete personal data provided by, or obtained about, the consumer;

4. 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, where the processing is carried out by automated means; and

5. opt out of the processing of the personal data for the purposes of "targeted advertising," the "sale of personal data," or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (i.e., controller decisions that result in providing or denying financial and lending services, housing, insurance, education, enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water).

Controllers must comply with any authenticated consumer requests to exercise these rights. Under the bill, an "authenticated" request is one verified through reasonable means that the consumer is the same consumer exercising the consumer rights with respect to the personal data at issue.

Under the bill, "targeted advertising" means displaying advertisements to a consumer where the advertisement 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. It does not include:

1. advertisements based on activities within a controller's own websites or online applications;

2. advertisements based on the context of a consumer's current search query, visit to a website, or online application;

3. advertisements directed to a consumer in response to the consumer's request for information or feedback; or

4. the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.

"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. It excludes the following:

1. disclosing personal data to a (a) processor that processes the personal data on the controller's behalf or (b) third party for purposes of providing a product or service the consumer requested; or

2. disclosing or transferring personal data to (a) the controller's affiliate or (b) a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction where the third party assumes control of all or part of the controller's assets; or

3. disclosing information that the consumer (a) intentionally made available to the general public through mass media, and (b) did not restrict to a specific audience.

Controller's Response

Except as otherwise provided by the bill, a controller must comply with a consumer's request to exercise these rights.

The bill requires a controller to respond to the consumer without undue delay, but within 45 days after receiving the request. The response period may be extended once for another 45 days when reasonably necessary considering the complexity and number of the consumer's requests. The controller must inform the consumer of any extension within the initial response period, together with the reason for extension.

If a controller declines to act on the consumer's request, the controller must inform the consumer without undue delay, but within 45 days after receiving the request. The notice must include the justification for declining to act and instructions on how to appeal the decision.

Under the bill, a controller must provide information in response to a consumer request for free and up to two times annually per consumer. If the consumer's request is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating why the request was manifestly unfounded, excessive, or repetitive.

If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with the request to initiate an action under this provision. The controller may request that the consumer provide additional information reasonably necessary to authenticate the consumer and his or her request.

The bill requires controllers to establish a process for a consumer to appeal the controller's refusal to act on a request within a reasonable time period after the consumer receives the decision. The appeals process must be conspicuously available and similar to the process for submitting requests to initiate action. Within 60 days after receiving an appeal, a controller must inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decision. If the controller denies the appeal, it must also provide the consumer with a method for contacting the attorney general and submitting a complaint.

§ 5 — CONTROLLERS

Requirements

The bill places numerous requirements on controllers. It requires them to:

1. limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purpose of data processing, as disclosed to the consumer and

2. establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

The bill provides that nothing in this provision should be construed to require a controller to provide a product or service that requires the consumer's personal data that the controller does not collect or maintain.

Prohibitions

Under the bill, controllers are also prohibited from processing:

1. personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer, except with the consumer's consent (i.e., a clear affirmative act signifying the consumer's agreement to allow the processing of their personal data, including by written statement, which may be electronic) or as allowed under the bill;

2. sensitive data concerning the consumer without their consent, or if the consumer is a known child, without processing the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.); and

3. personal data in violation of state and federal law that prohibit unlawful discrimination against consumers.

Under the bill, "sensitive data" means personal data that includes: (1) data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) processing genetic or biometric data in order to

uniquely identify a natural person; (3) personal data collected from a known child; or (4) precise geolocation data (i.e., information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identify the specific location of a natural person with precision and accuracy within a 1,750-foot radius. It does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment a utility uses).

Under the bill, "biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. It does not include physical or digital photographs, video or audio recordings, or data generated from these, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Discrimination

The bill prohibits controllers from discriminating against a consumer for exercising any rights the bill allows. This includes 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.

Difference in Goods or Services

The bill allows controllers to offer 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 his or her right to opt out or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Privacy Notice and Disclosure

The bill requires controllers to provide consumers with a reasonably accessible, clear, and meaningful privacy notice. The notice must include:

1. the categories of personal data processed by the controller;

2. the purpose for processing personal data;

3. how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision about the consumer's request;

4. the categories of personal data that the controller shares with third parties, if any; and

5. the categories of third parties, if any, with which the controller shares personal data.

Under the bill, if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the processing, as well as the way a consumer may exercise the right to opt out of the processing.

The controller must establish, and describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise the consumer rights the bill allows. The means must consider the ways the consumer normally interacts with the controller, the need for secure and reliable communications for these requests, and the ability of the controller to authenticate the consumer's identity. Controllers must not require a consumer to create a new account in order to make a request but may require them to use an existing account.

§ 6 — PROCESSORS

Controller's Instructions and Providing Assistance

The bill requires processors to adhere to the controller's instructions and assist the controller in meeting its obligations under the bill. This assistance must include considering the nature of processing and the information available to the processor by:

1. appropriate technical and organizational measures, as reasonably practicable, to fulfill the controller's obligation to

respond to consumer rights requests; and

2. assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a security breach of the processor's system.

Processors must also provide necessary information to enable the controller to conduct and document data protection assessments.

Contract

Under the bill, a contract between a controller and a processor must govern the processor's data processing procedures regarding processing performed on the controller's behalf. The contract is binding and must have clear instructions for processing data, the processing's nature and purpose, and both parties' rights and obligations.

The contract must also include requirements that the processor:

1. ensure that each person processing personal data is subject to a duty of confidentiality regarding the data;

2. at the controller's direction, delete or return all personal data to the controller as requested at the end of providing services, unless the law requires the personal data retention;

3. upon the controller's reasonable request, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations under the bill;

4. engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the processor's obligations regarding personal data; and

5. allow, and cooperate with, the controller or the controller's designated assessor to make reasonable assessments, or the processor may arrange for a qualified and independent assessor

to evaluate the processor's policies and technical and organizational measures regarding the bill's requirements, using an appropriate and accepted control standard or framework and assessment procedure for these assessments.

The bill states that nothing in this provision should be construed to relieve a controller or a processor from the liabilities imposed on it based on its role in the processing relationship.

Fact-based Determination for Controller

Under the bill, determining whether a person is acting as a controller or processor regarding a specific data process is a fact-based determination that depends on the context in which the data is processed. A processor that continues to adhere to a controller's instructions with a specific data processing remains a processor.

§ 7 — DATA PROTECTION ASSESSMENT

Assessment Requirements

The bill requires a controller to conduct and document a data protection assessment for (1) processing personal data for targeted advertising purposes, (2) selling personal data, (3) processing sensitive data, and (4) processing activities involving personal data that present a heightened risk of harm to consumers.

Controllers must also conduct an assessment for processing personal data for purposes of profiling, when the profiling presents a reasonably foreseeable risk of:

1. unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

2. financial, physical, or reputational injury to consumers;

3. a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where this intrusion would be offensive to a reasonable person; or

4. other substantial injury to consumers.

The bill defines "profiling" as any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Under the bill, data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the consumer's rights associated with the processing, as mitigated by the controller's safeguards. They must also take into account the use of de-identified data (as described below) and the consumer's reasonable expectations, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

The bill allows the attorney general to require a controller disclose and make available any data protection assessment that is relevant to his investigations. The attorney general may evaluate the assessment for compliance with the responsibilities the bill imposes. The assessments must be confidential and are exempt from disclosure under the Freedom of Information Act. Disclosure of the assessment pursuant to an attorney general's request does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information in it.

The bill allows a single data protection assessment to address a comparable set of processing operations that include similar activities. Assessments the controller conducts for the purposes of compliances with other laws or regulations may comply with this provision if the assessments have a reasonably comparable scope and effect.

The bill specifies that data protection assessment requirements apply to processing activities created or generated after January 1, 2023, and are not retroactive.

§ 8 — DE-IDENTIFIED DATA

Requirements

The bill requires any controller that possesses de-identified data to:

1. take reasonable measures to ensure the data cannot be associated with a natural person,

2. publicly commit to maintaining and using de-identified data without attempting to re-identify the data, and

3. contractually obligate any recipient of the de-identified data to comply with the bill's requirements.

Under the bill, "de-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person.

Applicability

The bill specifies that it should not be construed to (1) require a controller or processor to re-identify de-identified or pseudonymous data, or (2) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data. Additionally, it does not require a controller or processor to comply with an authenticated consumer rights request if the controller:

1. is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data,

2. does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer, and

3. does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted.

Pseudonymous Data

Under the bill, a consumer's rights do not apply to pseudonymous data when the controller is able to demonstrate any information needed to identify the consumer is kept separately and has effective technical and organizational controls that prevent the controller from accessing the information.

The bill defines "pseudonymous data" as personal data that cannot be attributed to a specific natural person without using additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

The bill requires a controller that discloses pseudonymous or de-identified data to exercise reasonable oversight to monitor compliance with any contractual commitments to which the data is subject. Controllers must take appropriate steps to address any such contractual breaches.

§ 9 — PROCESSING PERSONAL DATA FOR SPECIFIED PURPOSES

Ability to Comply With or Take Certain Other Actions

The bill specifies that nothing in it should be construed to restrict a controller's or processor's ability to:

1. comply with federal, state, or municipal ordinances or regulations or a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authorities;

2. cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;

3. investigate, establish, exercise, prepare for, or defend legal claims;

4. provide a product or service a consumer specifically requested;

5. perform a contract to which a consumer is a party, including by fulfilling written warranty terms;

6. take steps at the consumer's request before entering into a contract;

7. take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

8. 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 any such action;

9. engage in public- or peer-reviewed scientific or statistical research in the public interest that follows applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine (a) if deleting the information is likely to provide substantial benefits that do not exclusively benefit the controller, (b) the research's expected benefits outweigh the privacy risk, (c) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; or

10. assist another controller, processor, or third party with any obligations under the bill.

Ability to Collect, Use, or Retain Data

The bill also specifies the obligations it imposes on controllers or processors do not restrict the controller's or processor's ability to collect, use, or retain data to:

1. conduct internal research to develop, improve, or repair products, services, or technology;

2. effectuate a product recall;

3. identify and repair technical errors that impair existing or intended functionality; or

4. perform internal operations that are reasonably aligned with the consumer's expectations, reasonably anticipated based on the consumer's existing relationship with the controller, or compatible with processing data based on (a) providing a product or service the consumer specifically requested or (b) performing a contract to which the consumer is a party.

Evidentiary Privilege

Under the bill, the obligations imposed on controllers or processors do not apply where compliance would violate state evidentiary privilege. The bill should not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by state evidentiary privilege laws as a privileged communication.

Third-party Liability

Under the bill, controllers or processors that disclose personal data to a third party in compliance with the bill's requirements are not in violation of those provisions if a third-party controller or processor receives and processes the data in violation of those provisions. At the time of disclosure, the original controllers or processors must not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the bill is also not in violation for the controller's or processor's transgressions from receiving the personal data.

First Amendment Rights

The bill states that its provisions are not an obligation imposed on controllers and processors that adversely affects any individual's

rights or freedoms, such as exercising the right of free speech under the First Amendment of the U.S. Constitution. It also does not affect a person processing personal data for a purely personal or household activity.

Limitations on Processing Personal Data

The bill prohibits a controller from processing personal data for any purpose other than those expressly allowed under the bill. Controllers may process data to the extent the processing is (1) reasonably necessary and proportionate to the purposes of this provision and (2) adequate, relevant, and limited to what is necessary to the specific listed purpose. Personal data collected, used, or retained must consider the nature and purposes of these actions. The data is subject to reasonable administrative, technical, and physical measures to protect the personal data's confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers related to the collection, use, or retention of personal data.

Under the bill, if a controller processes personal data for a specified purpose through one of the exemptions listed above, the controller bears the burden of demonstrating that the processing qualifies under the exemption and complies with the bill's requirements for processing personal data.

The bill specifies that processing personal data for the purposes expressly identified in this provision does not solely make an entity a controller with respect to the processing.

§§ 10 & 11 — ATTORNEY GENERAL POWERS

Exclusive Authority

Under the bill, the attorney general has exclusive authority to enforce the bill's provisions by bringing an action in the state's name, or on behalf of state residents.

Notice

Under the bill, before initiating any actions the bill authorizes, the attorney general must provide a controller or processor with at least 30

days' written notice identifying the specific provisions the attorney general, on a consumer's behalf, alleges have been or are being violated.

Penalties

If the controller or processor:

1. cures the noticed violation in the provided noticed period and provides the attorney general an express written statement that the alleged violation has been cured and that no further violations occur, then no action for statutory damages will be initiated against them.

2. continues to violate the bill's provisions in breach of an express written statement provided to the consumer, the attorney general may initiate a civil action in Superior Court and seek damages of up to $7,500 for each violation.

The bill specifies that none of its provisions should be construed as providing the basis for, or be subject to, a private right of action for violations under the bill or any other law.

Under the bill, any controller or processor that violates the bill's provisions is liable for a civil penalty of up to $7,500 per violation. The attorney general may also recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, of any action initiated under the bill.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 18 Nay 0 (03/23/2021)