OLR Bill Analysis

sSB 6 (File 238, as amended by Senate "A")*

AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

SUMMARY

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

1. sets 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. gives 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 controllers to conduct data protection assessments;

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

5. deems violations to be Connecticut Unfair Trade Practices Act (CUTPA) violations.

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 from its requirements (1) various entities, including state and local governments, 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.

The bill also establishes a task force to, among other things, study Health Insurance Portability and Accountability Act (HIPAA)-adjacent data and other topics on data privacy and make recommendations to the General Law Committee by January 1, 2023.

*Senate Amendment "A" (1) increases an applicability threshold from 75,000 to 100,000 consumers; (2) modifies exemptions to include health plans, health care clearinghouses, health care providers, and other associates rather than hospitals; (3) exempts a controller from confirming a consumer's personal data is being processed if it requires revealing a trade secret; (4) specifies that controllers do not need to authenticate opt-out requests and allows them to deny fraudulent opt-out requests; (5) lowers the prohibited age, from 18 to 16, for targeted advertising or personal data sales without the consumer's consent; (6) eliminates the opt-out provision that generally prohibited controllers from selling personal data under a club program; (7) renames the working group as a task force and expands the scope of the required study; and (8) makes other minor, technical, and conforming changes.

EFFECTIVE DATE: July 1, 2023, except the task force provision is effective upon passage.

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

The bill's requirements generally apply to individuals and entities that do business in Connecticut or produce products or services targeting Connecticut residents and, during the preceding year, controlled or processed personal data of at least:

1. 100,000 consumers, excluding personal data controlled or processed solely for completing a payment transaction, or

2. 25,000 consumers and derived more than 25% of their gross revenue from selling personal data.

The bill defines a consumer as a state resident but excludes an individual acting (1) in a commercial or employment context or (2) as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that person's role with the entity.

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

"Personal data" is any information that is linked, or reasonably linkable, to an identified or identifiable individual excluding de-identified data or publicly available information. "Publicly available information" means information that (1) is lawfully made available through federal, state, or municipal government records, or widely distributed media and (2) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

"Process" or "processing" means any manual or automatic operation or set of operations performed 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. state body, authority, board, bureau, commission, district, or agency or those of its political subdivisions;

2. federally tax exempt nonprofit organization;

3. private or public higher education institution;

4. national securities association that is registered under federal law;

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

6. covered entities or business associates, as defined in HIPAA regulations (e.g., health plans, health care clearinghouses, and health care providers).

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. patient identifying information for purposes of a federal law on substance use disorder treatment (42 U.S.C. 290dd-2);

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

4. 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;

5. 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 for protecting human subjects the bill exempts above, or other research conducted in accordance with applicable law (45 C.F.R. 164.501);

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

7. patient safety work product for the purposes of patient safety organizations under state law (CGS § 19a-127o) and the federal Patient Safety and Quality Improvement Act (42 U.S.C. 299b-21 et seq.);

8. 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;

9. information originating from and intermingled to be indistinguishable with, or treated in the same manner as, other exempt information under the bill maintained by a covered entity (e.g., health care providers and plans) or business associate, program, or qualified service organization, as specified in a federal law related to substance use disorder treatment (42 U.S.C. 290dd-2);

10. information used for public health activities and purposes as authorized by HIPAA, community health activities, and population health activities;

11. 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.);

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

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

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

15. 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 these purposes; or (c) that is necessary to retain to administer benefits for another individual whose data is HIPAA-protected; and

16. personal data collected, processed, sold, or disclosed in relation to price, route, or service, as used in the federal Airline Deregulation Act (49 U.S.C. 40101 et seq.), by an air carrier subject to the act, to the extent the bill is preempted by the Airline Deregulation Act (49 U.S.C. 41713).

Parental Consent Exemption

The bill deems controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (COPPA) (15 U.S.C. 6501 et seq.) compliant with any obligation to obtain parental consent under the bill. Under the bill, COPPA includes the regulations, rules, guidance, and exemptions adopted under the act.

§ 4 — CONSUMER RIGHTS

With certain exceptions, 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, unless the confirmation or access would require the controller to reveal a trade secret;

2. correct inaccuracies in the consumer's personal data, considering its nature and the reason it is being processed;

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

4. obtain a copy of the consumer's personal data processed by 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, as long as the controller is not required to reveal any trade secret; and

5. opt out of personal data processing for the purposes of (a) "targeted advertising," (b) the "sale of personal data," except as allowed under the bill for opting out of club programs (e.g., loyalty program § 6), or (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer (i.e., controller decisions that result in providing or denying financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services).

Related Definitions. Under existing law and the bill, a "trade secret" is information, including a formula, pattern, compilation, program, device, method, technique, process, drawing, cost data, or customer list that (1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other individuals who can obtain economic value from its disclosure or use, and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

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 individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Targeted advertising" means displaying specific advertisements to a consumer based on personal data obtained or inferred 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. processing personal data solely measuring or reporting advertising frequency, performance, or reach.

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

1. disclosing personal data (a) to a processor that processes the personal data on the controller's behalf, (b) to a third party for purposes of providing a product or service the consumer requested, or (c) where the consumer directs the controller to disclose the data or intentionally uses the controller to interact with a third party;

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

3. disclosing personal data 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 the rights described above.

The bill requires a controller to respond to the consumer without undue delay, but within 45 days after receiving the request. The controller may extend the response period for 45 more days when

reasonably necessary considering the complexity and number of the consumer's requests. The controller must tell the consumer about any extension within the initial response period and the reason for it.

If a controller declines to act on the consumer's request, the controller must tell 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 give information in response to a consumer request for free, once per consumer during any 12-month period. 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 showing why the request was manifestly unfounded, excessive, or repetitive.

If a controller, using commercially reasonable efforts, cannot authenticate a consumer's request to confirm, correct, delete, or obtain a copy of the personal data processed, the controller is not required to comply with the request to initiate an action under this provision. The controller must notify the consumer that it is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the consumer and his or her request.

Under the bill, a controller is not be required to authenticate an opt-out request but may deny it if the controller has good faith, reasonable and documented belief the request is fraudulent. If a controller denies a fraudulent request, it must send notice to the requester by disclosing why it believed the request was fraudulent and that it did not comply with the request.

Under the bill, a controller that obtained personal data about a consumer from a source other than the consumer is deemed in compliance with a consumer's request to delete the data if the controller:

1. retains a record of the deletion request and the minimum data needed for ensuring the consumer's personal data remains

deleted from the controller's records and does not use the retained data for any other purpose pursuant to the bill's requirements, or

2. opts the consumer out of the personal data processing for any purposes, except those the bill exempts from its requirements.

The bill requires controllers to set up 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 in response to the appeal, including a written explanation of the reasons for the decision. If the controller denies the appeal, it must also give the consumer a specified method for contacting the attorney general and submitting a complaint.

§§ 4 & 5 — ACTING ON A CONSUMER'S BEHALF

The bill allows a consumer to exercise certain rights under this provision by a secure and reliable means set by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent to exercise his or her right to opt out of the processing of his or her personal data for purposes of targeted advertising, the sale of personal data, or automatic profiling.

The consumer may designate the authorized agent using technology indicating the consumer's intent to opt out of the processing, such as an Internet link or browser setting, browser extension, or global device setting. The bill requires a controller to comply with an opt-out request from an authorized agent if the controller can verify, with commercially reasonable effort, the consumer's identity and the authorized agent's authority to act on the consumer's behalf.

Children and Individuals Subject to Protective Arrangements

In the case of processing a child's personal data, the bill allows a parent or legal guardian to exercise the above opt-out rights on the

child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship, or other protective arrangement, the consumer's guardian or conservator may exercise these rights on the consumer's behalf.

§ 6 — CONTROLLERS

Requirements

The bill requires controllers to do the following:

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

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; and

3. offer an effective mechanism for a consumer to revoke his or her consent that is at least as easy as the mechanism the consumer used to give consent. When consent is revoked, the controller must stop processing the data as soon as practicable, but within 15 days after getting the request.

Prohibitions

The bill prohibits controllers from processing the following:

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 or as allowed under the bill;

2. sensitive data about the consumer without consent, or if the consumer is a known child (i.e., someone younger than age 13), without processing the data in accordance with COPPA;

3. personal data in violation of state and federal laws that prohibit

unlawful discrimination against consumers; and

4. a consumer's personal data for targeted advertising or selling the data without the consumer's consent, where a controller has actual knowledge of, and willfully disregards, that the consumer is ages 13-15.

Related Definitions. Under the bill, a consumer's consent means a clear affirmative act signifying the consumer's informed agreement to allow the processing of his or her personal data, including by written statement, which may be electronic. It does not include (1) acceptance of a general or broad term of use or similar document that contains personal data processing descriptions along with other, unrelated information; (2) hovering over, muting, pausing, or closing a given piece of content; or (3) agreement obtained through the use of dark patterns.

A "dark pattern" (1) is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and (2) includes any practice the Federal Trade Commission refers to as "dark pattern."

Under the bill, "sensitive data" means personal data that includes: (1) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; (2) processing genetic or biometric data in order to uniquely identify an individual; (3) personal data collected from a known child; or (4) precise geolocation data.

Under the bill, "biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics used to identify a specific individual. It does not include physical or digital or physical photographs, video or audio recordings, or data generated from these, unless the data is generated to identify a specific individual.

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.

Goods or Services a Controller Does Not Collect

The bill specifies that a controller is not required to provide a product or service that requires a consumer's personal data that the controller does not collect or maintain.

Difference in Goods or Services (e.g., Club Program)

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 offer is connected with 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 the controller processes;
2. the purpose for processing personal data;
3. how consumers may exercise their data privacy rights, including how to 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;
5. the categories of third parties, if any, with which the controller shares personal data; and
6. an active e-mail address or other online mechanism that the consumer can use to contract the controller.

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 how a consumer can exercise his or her opt-out rights.

The controller must set up, 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 how the consumer normally interacts with the controller, the need for secure and reliable communications for these requests, and the ability of the controller to verify the consumer's identity.

Opt-Outs

Under the bill, the secure and reliable means described above must include providing a clear and conspicuous link on the controller's website to a website that enables a consumer or the consumer's agent to opt out of the targeted advertising or sale of the consumer's personal data.

By January 1, 2025, consumers must be allowed to opt out of any processing of the consumer's personal data for targeted advertising or personal data sales. The opt-out preference must be sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of the processing or sale.

The bill requires that the platform, technology, or mechanism:

1. not unfairly disadvantage another controller;

2. not use a default setting, but instead require the consumer to affirmatively and freely give an unambiguous choice to opt out of any processing of his or her personal data that the bill regulates;

3. be consumer-friendly and easy to use by the average consumer;

4. be as consistent as possible with other similar platforms,

technologies, or mechanisms required by federal or state law or regulation; and

5. enable the controller to accurately determine whether the consumer is a Connecticut resident and whether the consumer has made a legitimate request to opt out of any sale of his or her personal data or targeted advertising.

If a consumer's opt out of targeted advertising or the sale of their personal data conflicts with his or her existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller must comply with the consumer's opt-out preference. The controller may notify the consumer about the conflict and provide the consumer the choice to confirm the privacy setting or participation in the program.

If a controller responds to a consumer's opt-out request by informing the consumer of a charge for using any product or service, the controller must present the terms of any financial incentive offered for retaining, using, selling, or sharing the consumer's personal data.

Under the bill, controllers must not require a consumer to create a new account in order to make a request, but can require them to use an existing account.

§ 7 — PROCESSORS

Controller's Instructions and Providing Assistance

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

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

2. helping the controller meet its obligations in relation to the

security of processing the personal data and in relation to the notification about a security breach of the processor's system under the state's existing data security law.

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

Contracts

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

The contract must also require the processor to do the following:

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 that it be retained;

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. after providing the controller an opportunity to object, 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. (In this case, the processor must give a report of the assessment to the controller on request.)

The bill specifies that these requirements should not be construed as relieving a controller or a processor from liability 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 for a specific data process is a fact-based determination that depends on the context in which the data is processed.

A person that is not limited in processing personal data under a controller's instructions, or that fails to adhere to these instructions, is a controller and not a processor with respect to that specific data processing. A processor that continues to adhere to a controller's instructions with a specific data processing remains a processor. If a processor begins, alone or with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to that processing and may be subject to the bill's enforcement actions.

§ 8 — DATA PROTECTION ASSESSMENT

Assessment Requirements

The bill requires controllers to conduct certain data protection assessments as described below. It specifies that these requirements apply to processing activities created or generated after July 1, 2023, and are not retroactive.

Specifically, the bill requires controllers to conduct and document a data protection assessment for each of their processing activities that presents a heighted risk of harm to a consumer. This includes (1) processing personal data for targeted advertising purposes, (2) selling personal data, and (3) processing sensitive data.

Controllers must also conduct an assessment for processing personal

data used for 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, 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.

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 a single data protection assessment to address a comparable set of processing operations that include similar activities. If a controller conducts an assessment to comply with another applicable law or regulation, that assessment is deemed to satisfy the bill's requirements if it is reasonably similar in scope and effect.

Disclosure to Attorney General

The bill allows the attorney general to require a controller to disclose and make available any data protection assessment relevant to his investigations. The attorney general may evaluate the assessment for compliance with the responsibilities the bill imposes. The assessments are confidential and exempt from disclosure under the state's Freedom of Information Act. To the extent any information in an assessment disclosed to the attorney general includes information subject to

attorney-client privilege or work product protection, the bill specifies that a disclosure does not constitute a waiver of the privilege or protection.

§ 9 — 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 an individual,

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 used to infer information about, or otherwise be linked to, a specific individual or their device. To be de-identified, a controller that possesses the data must (1) take reasonable measures to ensure the data cannot be associated with the individual, (2) publicly commit to process the data only in a de-identified fashion and not attempt to re-identify the data, and (3) contractually obligate anyone receiving the data to satisfy these requirements.

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.

Under the bill, an "authenticated" request is one made using reasonable means to determine that a request to exercise any of the rights afforded under the bill is being made by, or on behalf of, the consumer who is entitled to exercise these consumer rights with respect to the personal data at issue.

Pseudonymous Data

Under the bill, a consumer's rights under the bill specified above (see § 4) 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 it.

The bill defines "pseudonymous data" as personal data that cannot be attributed to a specific individual 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 individual.

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.

§ 10 — PROCESSING PERSONAL DATA FOR SPECIFIED PURPOSES

Ability to Comply With or Take Certain Other Actions

The bill specifies that nothing in its provisions 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 an individual 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 if (a) 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, and (c) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

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

11. process personal data for public interest reasons in public health, community health, or population health, but solely to the extent that the processing is (a) subject to suitable and specific measures to safeguard the consumer's rights whose personal data is being processed, and (b) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

Ability to Collect, Use, or Retain Data. The bill also specifies that the obligations it imposes on controllers or processors do not restrict their ability to collect, use, or retain data for internal use to:

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

2. recall products;

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 if doing so would make them 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 under the bill's requirements are not responsible for violations by them.

At the time of disclosure, the original controllers or processors must not have had actual knowledge that the recipient would violate the bill. 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.

First Amendment Rights. The bill states that its provisions are not to be construed to: (1) impose an obligation on a controller or processor that adversely affects any person, including his or her rights to freedom of speech or freedom of the press guaranteed under the First Amendment of the U.S. Constitution or the state law protecting disclosure of information by news media (CGS § 52-146t). It also does not affect a person processing personal data for a purely personal or household activity.

Limitations on Processing Personal Data. Under the bill, controllers may process data to the extent the processing is (1) reasonably necessary and proportionate to the purposes listed above (e.g., for internal research or effectuate product recall) and (2) adequate, relevant, and limited to what is necessary to the specific listed purpose. When applicable, personal data collected, used, or retained must consider the nature and purposes of these actions. The data must be subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers related to its collection, use, or retention.

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 showing that the processing (1) qualifies for an exemption

under the bill and (2) 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, on its own, make an entity a controller.

§ 11 — ATTORNEY GENERAL POWERS

Exclusive Authority

Under the bill and with certain exceptions, the attorney general has exclusive authority to enforce the bill's provisions. The bill establishes a grace period through December 31, 2024, during which the attorney general must give violators an opportunity to cure any violations. Beginning January 1, 2025, the bill grants the attorney general discretion in whether to provide an opportunity to correct an alleged 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 violation of the bill's requirements is an unfair trade practices violation (CUTPA) and is enforced solely by the attorney general, provided CUTPA's private right of action and class action provisions do not apply to the violation.

Notice and Opportunity to Correct Violations

From July 1, 2023, to December 31, 2024, the bill requires the attorney general, before initiating any action for a violation of the bill's provisions, to issue a notice of violation to the controller if he determines a cure is possible. If the controller fails to cure the violation within 60 days of receiving notice, the attorney general may bring an action.

Under the bill, by February 1, 2024, the attorney general must submit a report to the General Law Committee disclosing:

1. the number of notices of violations he issued,

2. the nature of each violation,

3. the number of violations cured within the 60-day period, and

4. any other matters he deems relevant.

Violations After January 1, 2025

Beginning on January 1, 2025, the attorney general may, in determining whether to give a controller or processor the opportunity to cure an alleged violation, consider (1) the number of violations, (2) the controller's or processor's size and complexity and the nature and extent of the controller's or processor's processing activities, (3) the substantial likelihood of injury to the public, (4) the safety of individuals or property, and (5) whether the alleged violation was likely caused by human or technical error.

§ 12 — TASK FORCE

By September 1, 2022, the bill requires the General Law Committee chairpersons to convene a task force to study:

1. information sharing among health care and social care providers and make recommendations to eliminate health disparities and inequities across sectors (as described in the Commission on Racial Equity and Public Health's authorizing statute);

2. algorithmic decision-making and make recommendations concerning the proper use of data to reduce bias in this decision-making;

3. possible legislation that would require an operator under COPPA to (a) upon a parent's request, delete a child's account and stop collecting, using, or maintaining, in retrievable form, the child's personal data on the operator's website or online service directed to children, and (b) provide parents with an accessible, reasonable, and verifiable means to make the request;

4. any means available to verify a child's age who creates a social media account;

5. issues concerning data colocation, including the bill's impact on

third parties that provide data storage and colocation services;

6. possible legislation that would expand the bill's applicability to include additional individuals or groups; and

7. other data privacy topics.

The General Law chairpersons must serve as the task force's chairpersons and jointly appoint its members. The members must include representatives from business, academia, consumer advocacy groups, small and large companies, the attorney general's office, and attorneys with privacy law expertise. The General Law Committee's administrative staff must serve as the task force's administrative staff.

By January 1, 2023, the bill requires the task force to submit a report on its findings and recommendations to the General Law Committee. The task force terminates when it submits the report or January 1, 2023, whichever is later.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 14 Nay 4 (03/15/2022)

Judiciary Committee

Joint Favorable
Yea 25 Nay 14 (04/11/2022)

Appropriations Committee

Joint Favorable
Yea 48 Nay 0 (04/18/2022)