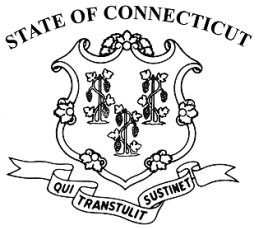

Substitute Senate Bill No. 3

Public Act No. 23-56

AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 42-515 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

As used in this section and sections 42-516 to 42-525, inclusive, as amended by this act, and section 2 of this act, unless the context otherwise requires:

(1) "Abortion" means terminating a pregnancy for any purpose other than producing a live birth.

[(1)**]** (2) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" **[**or**]** and "controlled" **[**means**]** mean (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

[(2)**]** (3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 42-518 is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

[(3)**]** (4) "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. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

[(4)**]** (5) "Business associate" has the same meaning as provided in HIPAA.

[(5)**]** (6) "Child" has the same meaning as provided in COPPA.

[(6)**]** (7) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

[(7)**]** (8) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or 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 individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(9) "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

(10) "Consumer health data controller" means any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.

[(8)**]** (11) "Controller" means **[**an individual**]** a person who, **[**or legal entity that,**]** alone or jointly with others, determines the purpose and means of processing personal data.

[(9)**]** (12) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

[(10)**]** (13) "Covered entity" has the same meaning as provided in HIPAA.

[(11)**]** (14) "Dark pattern" **[**(A)**]** means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and **[**(B)**]** includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

[(12)**]** (15) "Decisions that produce legal or similarly significant effects

concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

[(13)**]** (16) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(17) "Gender-affirming health care services" has the same meaning as provided in section 52-571n.

(18) "Gender-affirming health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

(19) "Geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary.

[(14)**]** (20) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

[(15)**]** (21) "Identified or identifiable individual" means an individual

who can be readily identified, directly or indirectly.

[(16)**]** (22) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(23) "Mental health facility" means any health care facility in which at least seventy per cent of the health care services provided in such facility are mental health services.

[(17)**]** (24) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

(25) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

[(18)**]** (26) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

[(19)**]** (27) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

[(20)**]** (28) "Process" **[**or**]** and "processing" **[**means**]** mean any 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.

[(21)**]** (29) "Processor" means **[**an individual**]** a person who **[**, or legal entity that,**]** processes personal data on behalf of a controller.

[(22)**]** (30) "Profiling" means 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.

[(23)**]** (31) "Protected health information" has the same meaning as provided in HIPAA.

[(24)**]** (32) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such 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.

[(25)**]** (33) "Publicly available information" means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(34) "Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning

(A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment, (B) a social, psychological, behavioral or medical intervention, (C) a surgery or procedure, including, but not limited to, an abortion, (D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion, (E) a bodily function, vital sign or symptom, (F) a measurement of a bodily function, vital sign or symptom, or (G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

(35) "Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(36) "Reproductive or sexual health facility" means any health care facility in which at least seventy per cent of the health care-related services or products rendered or provided in such facility are reproductive or sexual health care.

[(26)**]** (37) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or

other transaction, in which the third party assumes control of all or part of the controller's assets.

[(27)**]** (38) "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) consumer health data, (C) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, **[**(C)**]** (D) personal data collected from a known child, **[**or (D)**]** (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, or (F) precise geolocation data.

[(28)**]** (39) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

[(29)**]** (40) "Third party" means **[**an individual or legal entity**]** a person, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

[(30)**]** (41) "Trade secret" has the same meaning as provided in section 35-51.

Sec. 2. (NEW) (*Effective July 1, 2023*) (a) (1) Except as provided in

subsection (b) of this section, subsections (b) and (c) of section 42-517 of the general statutes, as amended by this act, and section 42-524 of the general statutes, as amended by this act, no person shall: (A) Provide any employee or contractor with access to consumer health data unless the employee or contractor is subject to a contractual or statutory duty of confidentiality; (B) provide any processor with access to consumer health data unless such person and processor comply with section 42-521 of the general statutes; (C) use a geofence to establish a virtual boundary that is within one thousand seven hundred fifty feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data; or (D) sell, or offer to sell, consumer health data without first obtaining the consumer's consent.

(2) Notwithstanding section 42-516 of the general statutes, the provisions of subsection (a) of this section, and the provisions of section 42-515, as amended by this act, and sections 42-517 to 42-525, inclusive, of the general statutes, as amended by this act, concerning consumer health data and consumer health data controllers, apply to persons that conduct business in this state and persons that produce products or services that are targeted to residents of this state.

(b) The provisions of subsection (a) of this section shall not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) person who has entered into a contract with any body, authority, board, bureau, commission, district or agency described in subdivision (1) of this subsection while such person is processing consumer health data on behalf of such body, authority, board, bureau, commission, district or agency pursuant to such contract; (3) institution of higher education; (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (5)

financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; (6) covered entity or business associate, as defined in 45 CFR 160.103; (7) tribal nation government organization; or (8) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

Sec. 3. Subsections (a) to (c), inclusive, of section 42-517 of the general statutes are repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) The provisions of sections 42-515 to 42-525, inclusive, as amended by this act, do not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) person who has entered into a contract with any body, authority, board, bureau, commission, district or agency described in subdivision (1) of this subsection while such person is processing consumer health data on behalf of such body, authority, board, bureau, commission, district or agency pursuant to such contract; (3) nonprofit organization; **[**(3)**]** (4) institution of higher education; **[**(4)**]** (5) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; **[**(5)**]** (6) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; **[**or (6)**]** (7) covered entity or business associate, as defined in 45 CFR 160.103; (8) tribal nation government organization; or (9) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(b) The following information and data is exempt from the provisions of sections 42-515 to 42-525, inclusive, as amended by this act, and

section 2 of this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of section 19a-127o and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health **[**care related**]** care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (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 bearing on 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 such

activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (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, consumer health data controller or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the **[**Airline Deregulation Act**]** Federal Aviation Act of 1958, 49 USC 40101 et seq., **[**as amended from time to time, by an air carrier subject to said act, to the extent sections 42-515 to 42-525, inclusive, are preempted by**]** and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(c) Controllers, **[**and**]** processors and consumer health data controllers that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act.

Sec. 4. Subsection (a) of section 42-520 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) A controller shall: (1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer; (2) except as otherwise provided in sections 42-515 to 42-525, inclusive, as amended by this act, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (3) 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; (4) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA; (5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers; (6) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and (7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, **[**and**]** or wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 42-515 to 42-525, inclusive,

as amended by this act, including 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.

Sec. 5. Section 42-524 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) Nothing in sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act shall be construed to restrict a controller's, **[**or**]** processor's or consumer health data controller's ability to: (1) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) cooperate with law enforcement agencies concerning conduct or activity that the controller, **[**or**]** processor or consumer health data controller reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations; (4) investigate, establish, exercise, prepare for or defend legal claims; (5) provide a product or service specifically requested by a consumer; (6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (7) take steps at the request of a consumer prior to entering into a contract; (8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; (9) 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; (10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the

deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller or consumer health data controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller or consumer health data controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; (11) assist another controller, processor, consumer health data controller or third party with any of the obligations under sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act; or (12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers, **[**or**]** processors or consumer health data controllers under sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act shall not restrict a controller's, **[**or**]** processor's or consumer health data controller's 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) 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 expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or consumer health data controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers, **[**or**]** processors or

consumer health data controllers under sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act shall not apply where compliance by the controller, [or] processor or consumer health data controller with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act shall be construed to prevent a controller, [or] processor or consumer health data controller from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller, [or] processor or consumer health data controller that discloses personal data to a processor or third-party controller in accordance with sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller, [or] processor or consumer health data controller disclosed such personal data, the disclosing controller, [or] processor or consumer health data controller did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller, [or] processor or consumer health data controller in compliance with sections 42-515 to 42-525, inclusive, as amended by this act, and section 2 of this act is likewise not in violation of said sections for the transgressions of the controller, [or] processor or consumer health data controller from which such third-party controller or processor receives such personal data.

(e) Nothing in sections 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this act shall be construed to: (1) Impose any obligation on a controller, [or] processor or consumer health data controller that adversely affects the rights or freedoms of any person,

including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t; or (2) apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed by a controller or consumer health data controller pursuant to this section may be processed to the extent that such processing is: (1) Reasonably necessary and proportionate to the purposes listed in this section; and (2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data.

(g) If a controller or consumer health data controller processes personal data pursuant to an exemption in this section, the controller or consumer health data controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller or consumer health data controller with respect to such processing.

Sec. 6. Section 42-525 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) The Attorney General shall have exclusive authority to enforce violations of sections 42-515 to 42-524, inclusive, as amended by this act,

and section 2 of this act.

(b) During the period beginning on July 1, 2023, and ending on December 31, 2024, the Attorney General shall, prior to initiating any action for a violation of any provision of sections 42-515 to 42-524, inclusive, as amended by this act, and section 2 of this act, issue a notice of violation to the controller or consumer health data controller if the Attorney General determines that a cure is possible. If the controller or consumer health data controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section. Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing: (1) The number of notices of violation the Attorney General has issued; (2) the nature of each violation; (3) the number of violations that were cured during the sixty-day cure period; and (4) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller, **[**or**]** processor or consumer health data controller the opportunity to cure an alleged violation described in subsection (b) of this section, consider: (1) The number of violations; (2) the size and complexity of the controller, **[**or**]** processor or consumer health data controller; (3) the nature and extent of the controller's, **[**or**]** processor's or consumer health data controller's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; **[**and**]** (6) whether such alleged violation was likely caused by human or technical error; and (7) the sensitivity of the data.

(d) Nothing in sections 42-515 to 42-524, inclusive, as amended by this act, or section 2 of this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or

any other law.

(e) A violation of the requirements of sections 42-515 to 42-524, inclusive, as amended by this act, or section 2 of this act shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced solely by the Attorney General, provided the provisions of section 42-110g shall not apply to such violation.

Sec. 7. (NEW) (*Effective July 1, 2024*) (a) For the purposes of this section:

(1) "Authenticate" means to use reasonable means and make a commercially reasonable effort to determine whether a request to exercise any right afforded under subsection (b) of this section has been submitted by, or on behalf of, the minor who is entitled to exercise such right;

(2) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(3) "Minor" means any consumer who is younger than eighteen years of age;

(4) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(5) "Social media platform" (A) means a public or semi-public Internet-based service or application that (i) is used by a consumer in this state, (ii) is primarily intended to connect and allow users to socially interact within such service or application, and (iii) enables a user to (I) construct a public or semi-public profile for the purposes of signing into and using such service or application, (II) populate a public list of other users with whom the user shares a social connection within such service or application, and (III) create or post content that is viewable by other users, including, but not limited to, on message boards, in chat rooms,

or through a landing page or main feed that presents the user with content generated by other users, and (B) does not include a public or semi-public Internet-based service or application that (i) exclusively provides electronic mail or direct messaging services, (ii) primarily consists of news, sports, entertainment, interactive video games, electronic commerce or content that is preselected by the provider or for which any chat, comments or interactive functionality is incidental to, directly related to, or dependent on the provision of such content, or (iii) is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program; and

(6) "Unpublish" means to remove a social media platform account from public visibility.

(b) (1) Not later than fifteen business days after a social media platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian to unpublish such minor's social media platform account, the social media platform shall unpublish such minor's social media platform account.

(2) Not later than forty-five business days after a social media platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian to delete such minor's social media platform account, the social media platform shall delete such minor's social media platform account and cease processing such minor's personal data except where the preservation of such minor's social media platform account or personal data is otherwise permitted or required by applicable law, including, but not limited to, sections 42-515 to 42-525, inclusive, of the general statutes, as amended by this act. A social media platform may extend such forty-five business day period by an additional forty-five business days if such extension is reasonably necessary considering the complexity and number of the consumer's requests, provided the social media platform

informs the minor or, if the minor is younger than sixteen years of age, such minor's parent or legal guardian within the initial forty-five business day response period of such extension and the reason for such extension.

(3) A social media platform shall establish, and shall describe in a privacy notice, one or more secure and reliable means for submitting a request pursuant to this subsection. A social media platform that provides a mechanism for a minor or, if the minor is younger than sixteen years of age, the minor's parent or legal guardian to initiate a process to delete or unpublish such minor's social media platform account shall be deemed to be in compliance with the provisions of this subsection.

(c) If a social media platform is unable to authenticate a request submitted under subsection (b) of this section, the social media platform shall (1) not be required to comply with such request, and (2) provide a notice to the consumer who submitted such request disclosing that such social media platform (A) is unable to authenticate such request, and (B) will not be able to authenticate such request until such consumer provides the additional information that is reasonably necessary to authenticate such request.

(d) Any violation of the provisions of this section shall constitute an unfair trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

Sec. 8. (NEW) (*Effective October 1, 2024*) For the purposes of this section and sections 9 to 13, inclusive, of this act:

(1) "Adult" means any individual who is at least eighteen years of age;

(2) "Consent" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(3) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(4) "Controller" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(5) "Heightened risk of harm to minors" means processing minors' personal data in a manner that presents any reasonably foreseeable risk of (A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (B) any financial, physical or reputational injury to minors, or (C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person;

(6) "HIPAA" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(7) "Minor" means any consumer who is younger than eighteen years of age;

(8) "Online service, product or feature" means any service, product or feature that is provided online. "Online service, product or feature" does not include any (A) telecommunications service, as defined in 47 USC 153, as amended from time to time, (B) broadband Internet access service, as defined in 47 CFR 54.400, as amended from time to time, or (C) delivery or use of a physical product;

(9) "Person" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(10) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(11) "Precise geolocation data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(12) "Process" and "processing" have the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(13) "Processor" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(14) "Profiling" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(15) "Protected health information" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(16) "Sale of personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(17) "Targeted advertising" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act; and

(18) "Third party" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act.

Sec. 9. (NEW) (*Effective October 1, 2024*) (a) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature. In any enforcement action brought by the Attorney General pursuant to section 13 of this act, there shall be a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with the provisions of section 10 of this act concerning data protection assessments.

(b) (1) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall: (A) Process any minor's personal data (i) for the purposes of (I) targeted advertising, (II) any sale of personal data, or (III) profiling in furtherance of any fully automated decision made by such controller that produces any legal or similarly significant effect concerning the provision or denial by such controller of any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services or access to essential goods or services, (ii) unless such processing is reasonably necessary to provide such online service, product or feature, (iii) for any processing purpose (I) other than the processing purpose that the controller disclosed at the time such controller collected such personal data, or (II) that is reasonably necessary for, and compatible with, the processing purpose described in subparagraph (A)(iii)(I) of this subdivision, or (iv) for longer than is reasonably necessary to provide such online service, product or feature; or (B) use any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature. The provisions of this subdivision shall not apply to any service or application that is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program.

(2) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers an online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall collect a minor's precise geolocation data unless: (A) Such precise geolocation data is reasonably necessary for the controller to provide such online service, product or feature and, if such data is necessary to provide such online service, product or feature, such controller may only collect such data for the

time necessary to provide such online service, product or feature; and (B) the controller provides to the minor a signal indicating that such controller is collecting such precise geolocation data, which signal shall be available to such minor for the entire duration of such collection.

(3) No controller shall engage in the activities described in subdivisions (1) and (2) of this subsection unless the controller obtains the minor's consent or, if the minor is younger than thirteen years of age, the consent of such minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time, shall be deemed to have satisfied any requirement to obtain parental consent under this subdivision.

(c) (1) No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall: (A) Provide any consent mechanism that is designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision-making or choice; or (B) except as provided in subdivision (2) of this subsection, offer any direct messaging apparatus for use by minors without providing readily accessible and easy-to-use safeguards to limit the ability of adults to send unsolicited communications to minors with whom they are not connected.

(2) The provisions of subparagraph (B) of subdivision (1) of this subsection shall not apply to services where the predominant or exclusive function is: (A) Electronic mail; or (B) direct messaging consisting of text, photos or videos that are sent between devices by electronic means, where messages are (i) shared between the sender and the recipient, (ii) only visible to the sender and the recipient, and (iii) not

posted publicly.

Sec. 10. (NEW) (*Effective October 1, 2024*) (a) Each controller that, on or after October 1, 2024, offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall conduct a data protection assessment for such online service, product or feature: (1) In a manner that is consistent with the requirements established in section 42-522 of the general statutes; and (2) that addresses (A) the purpose of such online service, product or feature, (B) the categories of minors' personal data that such online service, product or feature processes, (C) the purposes for which such controller processes minors' personal data with respect to such online service, product or feature, and (D) any heightened risk of harm to minors that is a reasonably foreseeable result of offering such online service, product or feature to minors.

(b) Each controller that conducts a data protection assessment pursuant to subsection (a) of this section shall: (1) Review such data protection assessment as necessary to account for any material change to the processing operations of the online service, product or feature that is the subject of such data protection assessment; and (2) maintain documentation concerning such data protection assessment for the longer of (A) the three-year period beginning on the date on which such processing operations cease, or (B) as long as such controller offers such online service, product or feature.

(c) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(d) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment

that would otherwise be conducted pursuant to this section.

(e) If any controller conducts a data protection assessment pursuant to subsection (a) of this section and determines that the online service, product or feature that is the subject of such assessment poses a heightened risk of harm to minors, such controller shall establish and implement a plan to mitigate or eliminate such risk.

(f) Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to the attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

Sec. 11. (NEW) (*Effective October 1, 2024*) (a) A processor shall adhere to the instructions of a controller, and shall: (1) Assist the controller in meeting the controller's obligations under sections 8 to 13, inclusive, of this act taking into account (A) the nature of the processing, (B) the information available to the processor by appropriate technical and organizational measures, and (C) whether such assistance is reasonably practicable and necessary to assist the controller in meeting such obligations; and (2) provide any information that is necessary to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall satisfy the requirements established in subsection (b) of section 42-521 of the general statutes.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 8 to 13, inclusive, of this act.

(d) Determining 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 upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 13 of this act.

Sec. 12. (NEW) (*Effective October 1, 2024*) (a) The provisions of sections 8 to 11, inclusive, and section 13 of this act shall not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time; (3) individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees; (4) national securities association that is registered under 15 USC 78o-3, as amended from time to time; (5) financial institution or data that is subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time; (6) covered entity or business associate, as defined in 45 CFR 160.103, as amended from time to time; (7) tribal nation government organization; or (8) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended

from time to time.

(b) The following information and data is exempt from the provisions of sections 8 to 11, inclusive, and section 13 of this act: (1) Protected health information; (2) patient-identifying information for the purposes of 42 USC 290dd-2, as amended from time to time; (3) identifiable private information for the purposes of the federal policy for the protection of human subjects under 45 CFR 46, as amended from time to time; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, as amended from time to time; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, as amended from time to time, or personal data used or shared in research, as defined in 45 CFR 164.501, as amended from time to time, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq., as amended from time to time; (7) patient safety work products for the purposes of section 19a-127o of the general statutes and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification under HIPAA; (9) information originating from and intermingled so as to be indistinguishable from, or information treated in the same manner as, information that is exempt under this subsection and maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (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 bearing on 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 such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (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 the emergency contact information of an individual under sections 8 to 11, inclusive, and section 13 of this act used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(c) No provision of this section or sections 8 to 11, inclusive, or section 13 of this act shall be construed to restrict a controller's or processor's ability to: (1) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry,

investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) 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; (4) investigate, establish, exercise, prepare for or defend legal claims; (5) take immediate steps to protect an interest that is essential for the life or physical safety of the minor or another individual, and where the processing cannot be manifestly based on another legal basis; (6) 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; (7) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller or processor, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller or processor has implemented reasonable safeguards to mitigate privacy risks associated with research, including, but not limited to, any risks associated with re-identification; (8) assist another controller, processor or third party with any obligation under sections 8 to 11, inclusive, or section 13 of this act; or (9) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the minor whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(d) No obligation imposed on a controller or processor under any

provision of sections 8 to 11, inclusive, or section 13 of this act shall be construed to restrict a controller's or processor's 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) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are (A) reasonably aligned with the expectations of a minor or reasonably anticipated based on the minor's existing relationship with the controller or processor, or (B) otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a minor.

(e) No controller or processor shall be required to comply with any provision of sections 8 to 11, inclusive, or section 13 of this act if compliance with such provision would violate an evidentiary privilege under the laws of this state, and no such provision shall be construed to prevent a controller or processor from providing, as part of a privileged communication, any personal data concerning a minor to any other person who is covered by such evidentiary privilege.

(f) No provision of sections 8 to 11, inclusive, or section 13 of this act shall be construed to: (1) Impose any obligation on a controller that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t of the general statutes; or (2) apply to any individual's processing of personal data in the course of such individual's purely personal or household activities.

(g) (1) Any personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (A) Reasonably necessary and proportionate to the purposes listed in this section; and (B) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section.

(2) Any controller that collects, uses or retains data pursuant to subsection (d) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to minors concerning such collection, use or retention of personal data.

(h) If any controller or processor processes personal data pursuant to an exemption established in subsections (a) to (g), inclusive, of this section, such controller or processor bears the burden of demonstrating that such processing qualifies for such exemption and complies with the requirements established in subsection (g) of this section.

Sec. 13. (NEW) (*Effective October 1, 2024*) (a) Any violation of the provisions of sections 8 to 12, inclusive, of this act shall constitute an unfair trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section or sections 8 to 12, inclusive, of this act shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

(b) (1) During the period beginning October 1, 2024, and ending December 31, 2025, if the Attorney General, in the Attorney General's discretion, determines that a controller or processor has violated any provision of sections 8 to 12, inclusive, of this act but may cure such alleged violation, the Attorney General shall provide written notice to such controller or processor, in a form and manner prescribed by the Attorney General and before the Attorney General commences any action to enforce such provision, disclosing such alleged violation and such provision.

(2) (A) Not later than thirty days after a controller or processor

receives a notice under subdivision (1) of this subsection, the controller or processor may send a notice to the Attorney General, in a form and manner prescribed by the Attorney General, disclosing that such controller or processor has: (i) Determined that such controller or processor did not commit the alleged violation of sections 8 to 12, inclusive, of this act; or (ii) cured such violation and taken measures that are sufficient to prevent further such violations.

(B) If the Attorney General receives a notice described in subparagraph (A) of this subdivision and determines, in the Attorney General's discretion, that the controller or processor that sent such notice did not commit the alleged violation or has cured such violation and taken the measures described in subparagraph (A)(ii) of this subdivision, such controller or processor shall not be liable for any civil penalty under subsection (a) of this section.

(C) Not later than February 1, 2026, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law. Such report shall disclose: (i) The number of notices the Attorney General has issued pursuant to subdivision (1) of this subsection; (ii) the number of violations that were cured pursuant to subparagraphs (A) and (B) of this subdivision; and (iii) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2026, the Attorney General may, in the Attorney General's discretion, provide to a controller or processor an opportunity to cure any alleged violation of the provisions of sections 8 to 12, inclusive, of this act in the manner described in subdivisions (1) and (2) of subsection (b) of this section. In determining whether to grant the controller or processor an opportunity to cure such alleged violation, the Attorney General may consider: (1) The number of such violations that such controller or processor is alleged to have committed; (2) the

size and complexity of such controller or processor; (3) the nature and extent of such controller's or processor's processing activities; (4) whether there exists a substantial likelihood that such alleged violation has caused or will cause public injury; (5) the safety of persons or property; (6) whether such alleged violation was likely caused by a human or technical error; and (7) the sensitivity of the data.

Sec. 14. Section 21a-435 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective January 1, 2024*):

As used in this section, **[**and**]** sections 21a-436 to 21a-439, inclusive, as amended by this act, and section 15 of this act:

(1) "Connecticut user" means a user who provides a Connecticut home address or zip code when registering with an online dating operator or a user who is known or determined by an online dating operator or its online dating platform to be in Connecticut at the time of registration;

(2) "Criminal background screening" means a name search for an individual's history of criminal convictions that is conducted by searching an (A) available and regularly updated government public record database that in the aggregate provides national coverage for searching an individual's history of criminal convictions; or (B) a regularly updated database maintained by a private vendor that provides national coverage for searching an individual's history of criminal convictions and sexual offender registries;

(3) "Criminal conviction" means a conviction for a crime in this state, another state, or under federal law;

(4) "Online dating" means the act of using a digital service to initiate relationships with other individuals for the purpose of romance, sex or marriage;

(5) "Online dating operator" means a person who operates a software application designed to facilitate online dating;

(6) "Online dating platform" means a digital service designed to allow users to interact through the Internet to participate in online dating; and

(7) "User" means an individual who uses the online dating services of an online dating operator.

Sec. 15. (NEW) (*Effective January 1, 2024*) (a) Each online dating operator that offers services to Connecticut users shall maintain an online safety center, which shall be reasonably designed to provide Connecticut users with resources concerning safe dating. Each online safety center maintained pursuant to this subsection shall provide: (1) An explanation of the online dating operator's reporting mechanism for harmful or unwanted behavior; (2) safety advice for use when communicating online and meeting in person; (3) a link to an Internet web site or a telephone number where a Connecticut user may access resources concerning domestic violence and sexual harassment; and (4) educational information concerning romance scams.

(b) Each online dating operator that offers services to Connecticut users shall adopt a policy for the online dating platform's handling of harassment reports by or between users.

Sec. 16. Section 21a-439 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective January 1, 2024*):

(a) The Department of Consumer Protection may issue fines of not more than twenty-five thousand dollars per violation, accept an offer in compromise, or take other actions permitted by the general statutes or the regulations of Connecticut state agencies if an online dating operator fails to comply with the provisions of sections 21a-435 to 21a-438, inclusive, as amended by this act, and section 15 of this act.

(b) The Commissioner of Consumer Protection, or the commissioner's designee, may conduct investigations and hold hearings on any matter under the provisions of this section, **[**and**]** sections 21a-435 to 21a-438, inclusive, as amended by this act, and section 15 of this act. The commissioner, or the commissioner's designee, may issue subpoenas, administer oaths, compel testimony and order the production of books, records and documents. If any person refuses to appear, to testify or to produce any book, record or document when so ordered, upon application of the commissioner or the commissioner's designee, a judge of the Superior Court may make such order as may be appropriate to aid in the enforcement of this section.

(c) The Attorney General, at the request of the commissioner or the commissioner's designee, may apply in the name of the state to the Superior Court for an order temporarily or permanently restraining and enjoining any person from violating any provision of this section, **[**and**]** sections 21a-435 to 21a-438, inclusive, as amended by this act, and section 15 of this act.

Sec. 17. Section 29-7b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) There shall be within the Department of Emergency Services and Public Protection a Division of Scientific Services. The Commissioner of Emergency Services and Public Protection shall serve as administrative head of such division, and may delegate jurisdiction over the affairs of such division to a deputy commissioner.

(b) The Division of Scientific Services shall provide technical assistance to law enforcement agencies in the various areas of scientific investigation. The division shall maintain facilities and services for the examination and analysis of evidentiary materials in areas including, but not limited to, chemistry, arson, firearms, questioned documents, microscopy, serology, toxicology, trace evidence, latent fingerprints,

impressions and other similar technology. The facilities, services and personnel of the division shall be available, without charge, to the Office of the Chief Medical Examiner and all duly constituted prosecuting, police and investigating agencies of the state.

(c) The Division of Scientific Services: (1) May investigate any physical evidence or evidentiary material related to a crime upon the request of any federal, state or local agency, (2) may conduct or assist in the scientific field investigation at the scene of a crime and provide other technical assistance and training in the various fields of scientific criminal investigation upon request, (3) shall assure the safe custody of evidence during examination, (4) shall forward a written report of the results of an examination of evidence to the agency submitting such evidence, (5) shall render expert court testimony when requested, and (6) shall conduct ongoing research in the areas of the forensic sciences. The Commissioner of Emergency Services and Public Protection or a director designated by the commissioner shall be in charge of the Division of Scientific Services operations and shall establish and maintain a system of case priorities and a procedure for submission of evidence and evidentiary security. The director of the Division of Scientific Services shall be in the unclassified service and shall serve at the pleasure of the commissioner.

(d) In accordance with the provisions of sections 4-38d, 4-38e and 4-39, all powers and duties of the Department of Public Health under the provisions of sections 14-227a, 14-227c, 15-140u and 21a-283 shall be transferred to the Division of Scientific Services within the Department of Emergency Services and Public Protection.

(e) There is established within the Division of Scientific Services the Connecticut Internet Crimes Against Children Task Force, which shall consist of affiliate law enforcement agencies in the state. The task force shall use state and federal moneys appropriated to it in a manner that is consistent with the duties prescribed in 34 USC 21114.

Approved June 26, 2023