CHAPTER 743jj

DATA PRIVACY AND SECURITY

Table of Contents

PART I

CONSUMER DATA PRIVACY AND ONLINE MONITORING

Sec. 42-515. *(See end of section for amended version and effective date.) Definitions. As used in this section and sections 42-516 to 42-526, inclusive, unless the context otherwise requires:

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

(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” and “controlled” 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.

(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.

(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.

(5) “Business associate” has the same meaning as provided in HIPAA.

(6) “Child” has the same meaning as provided in COPPA.

(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 general or broad terms of use or a 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.

(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.

(11) “Controller” means a person who, alone or jointly with others, determines the purpose and means of processing personal data.

(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.

(13) “Covered entity” has the same meaning as provided in HIPAA.

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

(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.

(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 52-571m.

(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.

(20) “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(21) “Identified or identifiable individual” means an individual who can be readily identified, directly or indirectly.

(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.

(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.

(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.

(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.

(28) “Process” and “processing” 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.

(29) “Processor” means a person who processes personal data on behalf of a controller.

(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.

(31) “Protected health information” has the same meaning as provided in HIPAA.

(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.

(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.

(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.

(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, (D) personal data collected from a known child, (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, or (F) precise geolocation data.

(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.

(40) “Third party” means 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.

(41) “Trade secret” has the same meaning as provided in section 35-51.

(P.A. 22-15, S. 1; P.A. 23-56, S. 1; 23-110, S. 1; 23-204, S. 207; P.A. 25-168, S. 286.)

*Note: On and after July 1, 2026, this section, as amended by section 5 of public act 25-113, is to read as follows:

“Sec. 42-515. Definitions. As used in this section and sections 42-516 to 42-526, inclusive, unless the context otherwise requires:

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

(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” and “controlled” 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.

(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.

(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 are generated to identify a specific individual.

(5) “Business associate” has the same meaning as provided in HIPAA.

(6) “Child” has the same meaning as provided in COPPA.

(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 general or broad terms of use or a 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.

(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 organization 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 organization 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, diagnosis or status, 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.

(11) “Controller” means a person who, alone or jointly with others, determines the purpose and means of processing personal data.

(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.

(13) “Covered entity” has the same meaning as provided in HIPAA.

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

(15) “Decision that produces any legal or similarly significant effect” means any decision made by the controller, or on behalf of the controller, that results in the provision or denial by the controller of any financial or lending service, any housing, any insurance, any education enrollment or opportunity, any criminal justice, any employment opportunity or any health care service.

(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.

(20) “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(21) “Identified or identifiable individual” means an individual who can be readily identified, directly or indirectly.

(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.

(24) “Neural data” means any information that is generated by measuring the activity of an individual's central nervous system.

(25) “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.

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

(27) “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.

(28) “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.

(29) “Process” and “processing” 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.

(30) “Processor” means a person who processes personal data on behalf of a controller.

(31) “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.

(32) “Protected health information” has the same meaning as provided in HIPAA.

(33) “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 are not attributed to an identified or identifiable individual.

(34) “Publicly available information” (A) means information that (i) is lawfully made available from federal, state or municipal government records, or (ii) a controller has a reasonable basis to believe (I) a consumer has lawfully made available to the general public, or (II) has been lawfully made available to the general public from widely distributed media, and (B) does not include any biometric data that can be associated with a specific consumer and were collected without the consumer's consent.

(35) “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.

(36) “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.

(37) “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.

(38) “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.

(39) “Sensitive data” means personal data that includes (A) data revealing (i) racial or ethnic origin, (ii) religious beliefs, (iii) a mental or physical health condition, diagnosis, disability or treatment, (iv) sex life, sexual orientation or status as nonbinary or transgender, or (v) citizenship or immigration status, (B) consumer health data, (C) genetic or biometric data or information derived therefrom, (D) personal data collected from an individual the controller has actual knowledge, or wilfully disregards, is a child, (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, (F) precise geolocation data, (G) neural data, (H) a consumer's financial account number, financial account log-in information or credit card or debit card number that, in combination with any required access or security code, password or credential, would allow access to a consumer's financial account, or (I) government-issued identification number, including, but not limited to, Social Security number, passport number, state identification card number or driver's license number, that applicable law does not require to be publicly displayed.

(40) “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.

(41) “Third party” means 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.

(42) “Trade secret” has the same meaning as provided in section 35-51.”

(P.A. 22-15, S. 1; P.A. 23-56, S. 1; 23-110, S. 1; 23-204, S. 207; P.A. 25-168, S. 286; 25-113, S. 5.)

History: P.A. 22-15 effective July 1, 2023; P.A. 23-56 added reference to Sec. 42-526 in introductory language, added new Subdiv. (1) defining “abortion”, redesignated existing Subdivs. (1) to (7) as Subdivs. (2) to (8), added new Subdivs. (9) and (10) defining “consumer health data” and “consumer health data controller”, respectively, redesignated existing Subdivs. (8) to (13) as Subdivs. (11) to (16), amended redesignated Subdiv. (11) by substituting “a person who,” for “an individual who, or legal entity that,”, amended redesignated Subdiv. (14) by deleting Subpara. designators (A) and (B), added new Subdivs. (17) to (19) defining “gender-affirming health care services”, “gender-affirming health data” and “geofence”, respectively, redesignated existing Subdivs. (14) to (16) as Subdivs. (20) to (22), added new Subdiv. (23) defining “mental health facility”, redesignated existing Subdiv. (17) as Subdiv. (24), added new Subdiv. (25) defining “person”, redesignated existing Subdivs. (18) to (25) as Subdivs. (26) to (33), amended redesignated Subdiv. (29) by substituting “a person who” for “an individual who, or legal entity that,”, added Subdivs. (34) to (36) defining “reproductive or sexual health care”, “reproductive or sexual health data” and “reproductive or sexual health facility”, respectively, redesignated existing Subdivs. (26) to (30) as Subdivs. (37) to (41), amended redesignated Subdiv. (38) by adding Subpara. (B), redesignating existing Subparas. (B) and (C) as Subparas. (C) and (D), adding Subpara. (E) and redesignating existing Subpara. (D) as Subpara. (F), amended redesignated Subdiv. (40) by substituting “a person” for “an individual or legal entity”, and made technical and conforming changes throughout, effective July 1, 2023; P.A. 23-110 made technical changes in Subdiv. (6), effective July 1, 2023; P.A. 23-204 changed effective date of P.A. 23-56, S. 1, from July 1, 2023, to October 1, 2023, effective June 12, 2023; P.A. 25-113 amended Subdivs. (8) and (9) by redefining “consumer” and “consumer health data”, amended Subdiv. (15) by replacing definition of “decisions that produce legal or similarly significant effects concerning the consumer” with definition of “decision that produces any legal or similarly significant effect”, added new Subdiv. (24) defining “neural data”, redesignated existing Subdivs. (24) to (41) as Subdivs. (25) to (42), amended redesignated Subdivs. (34) and (39) by redefining “publicly available information” and “sensitive data”, and made technical changes in Subdiv. (4) and redesignated Subdiv. (33), effective July 1, 2026; P.A. 25-168 amended Subdiv. (17) by substituting Sec. 52-571m for repealed Sec. 52-571n, effective July 1, 2025.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-516. *(See end of section for amended version and effective date.) Applicability. The provisions of sections 42-515 to 42-525, inclusive, apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year: (1) Controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.

(P.A. 22-15, S. 2.)

*Note: On and after July 1, 2026, this section, as amended by section 6 of public act 25-113, is to read as follows:

“Sec. 42-516. Applicability. The provisions of sections 42-515 to 42-525, inclusive, apply to persons that: (1) Conduct business in this state, or produce products or services that are targeted to residents of this state, and during the preceding calendar year controlled or processed the personal data of not fewer than thirty-five thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; (2) control or process consumers' sensitive data, excluding personal data controlled or processed solely for the purposes of completing a payment transaction; or (3) offer consumers' personal data for sale in trade or commerce.”

(P.A. 22-15, S. 2; P.A. 25-113, S. 6.)

History: P.A. 22-15 effective July 1, 2023; P.A. 25-113 substantially amended provisions including by reducing threshold in Subdiv. (1) from not fewer than 100,000 consumers to not fewer than 35,000 consumers, deleting former Subdiv. (2) and adding new Subdiv. (2) re sensitive data and Subdiv. (3) re personal data offered for sale in trade or commerce, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-517. *(See end of section for amended versions of subsections (a) and (b) and effective date.) Exemptions. *(a) The provisions of sections 42-515 to 42-525, inclusive, 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; (4) institution of higher education; (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; (6) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; (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 42-526, inclusive: (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 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 42-526, inclusive, 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) Controllers, 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 42-526, inclusive.

(P.A. 22-15, S. 3; P.A. 23-56, S. 3; 23-204, S. 207.)

*Note: On and after July 1, 2026, subsections (a) and (b) of this section, as amended by section 7 of public act 25-113, are to read as follows:

"(a) The provisions of sections 42-515 to 42-525, inclusive, 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; (4) candidate committee, national committee, party committee or political committee, as such terms are defined in section 9-601; (5) institution of higher education; (6) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (7) covered entity or business associate, as defined in 45 CFR 160.103; (8) tribal nation government organization; (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; (10) insurer, as defined in section 38a-1, or its affiliate, fraternal benefit society, within the meaning of section 38a-595, health carrier, as defined in section 38a-591a, insurance-support organization, as defined in section 38a-976, or insurance agent or insurance producer, as such terms are defined in section 38a-702a; (11) bank, Connecticut credit union, federal credit union, out-of-state bank or out-of-state credit union, or any affiliate or subsidiary thereof, as such terms are defined in section 36a-2, that (A) is only and directly engaged in financial activities as described in 12 USC 1843(k), (B) is regulated and examined by the Department of Banking or an applicable federal bank regulatory agency, and (C) has established a program to comply with all applicable requirements established by the Banking Commissioner or the applicable federal bank regulatory agency concerning personal data; or (12) agent, broker-dealer, investment adviser or investment adviser agent, as such terms are defined in section 36b-3, who is regulated by the Department of Banking or the Securities and Exchange Commission.

(b) The following information and data are exempt from the provisions of sections 42-515 to 42-526, inclusive: (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) personal data for purposes of 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 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 are collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 42-515 to 42-526, inclusive, used for emergency contact purposes, or (C) that are 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; (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; (17) data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time; and (18) information included in a limited data set, as described in 45 CFR 164.514(e), as amended from time to time, to the extent such information is used, disclosed and maintained in the manner specified in 45 CFR 164.514(e), as amended from time to time."

(P.A. 22-15, S. 3; P.A. 23-56, S. 3; 23-204, S. 207; P.A. 25-113, S. 7.)

History: P.A. 22-15 effective July 1, 2023; P.A. 23-56 amended Subsec. (a) by adding new Subdiv. (2) re contractors of persons described in Subdiv. (1), redesignating existing Subdivs. (2) to (6) as Subdivs. (3) to (7) and adding Subdivs. (8) and (9) re tribal nation government organizations and air carriers, respectively, amended Subsec. (b) by adding references to Sec. 42-526 in introductory language and Subdiv. (15)(B), adding "consumer health data controller" to Subdiv. (15)(A) and substituting "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" for "Airline Deregulation Act, 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 are preempted by the Airline Deregulation Act, 49 USC 41713, as amended from time to time" in Subdiv. (16), amended Subsec. (c) by adding "and consumer health data controllers" and reference to Sec. 42-526, and made technical and conforming changes throughout, effective July 1, 2023; P.A. 23-204 changed effective date of P.A. 23-56, S. 3, from July 1, 2023, to October 1, 2023, effective June 12, 2023; P.A. 25-113 amended Subsec. (a) by adding new Subdiv. (4) re candidate committee, national committee, party committee or political committee, redesignating existing Subdivs. (4) and (5) as Subdivs. (5) and (6), deleting former Subdiv. (6) re financial institution or data subject to Title V of Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and adding new Subdivs. (10) to (12) re insurer, affiliate, fraternal benefit society, health carrier, insurance-support organization, insurance agent and insurance producer, bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state credit union, affiliate and subsidiary and agent, broker-dealer, investment adviser and investment adviser agent, amended Subsec. (b) by adding "personal data for purposes of" in Subdiv. (5) and adding Subdivs. (17) and (18) re data subject to Title V of Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and information included in limited data set, and made technical and conforming changes in Subsecs. (a) and (b), effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-518. *(See end of section for amended version and effective date.) Consumers' rights. Compliance by Controllers. Appeals. (a) A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (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, provided such controller shall not be required to reveal any trade secret; and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 42-520, or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 42-519 to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer 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 guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(c) Except as otherwise provided in sections 42-515 to 42-525, inclusive, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a

request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (3) of subsection (a) of this section by (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to the provisions of sections 42-515 to 42-525, inclusive, or (B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of sections 42-515 to 42-525, inclusive.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

(P.A. 22-15, S. 4.)

*Note: On and after July 1, 2026, this section, as amended by section 8 of public act 25-113, is to read as follows:

“Sec. 42-518. Consumers' rights. Compliance by Controllers. Appeals. (a) A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, including, but not limited to, any inferences about the consumer derived from such personal data and whether a controller or processor is processing a consumer's personal data for the purposes of profiling to make a decision that produces any legal or similarly significant effect concerning a consumer, unless such confirmation or access would require the controller to reveal a trade secret or the controller is prohibited from disclosing such personal data under subsection (e) of this section; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (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, provided such controller shall not be required to reveal any trade secret; (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subdivision (2) of subsection (a) of section 42-520, or (C) profiling in furtherance of any automated decision that produces any legal or similarly significant effect concerning the consumer; (6) if the consumer's personal data were processed for the purposes of profiling in furtherance of any automated decision that produced any legal or similarly significant effect concerning the consumer, and if feasible, (A) question the result of such profiling, (B) be informed of the reason that such profiling resulted in such decision, (C) review the consumer's personal data that were processed for the purposes of such profiling, and (D) if the profiling decision concerned housing, taking into account the nature of the personal data and the purposes for which such personal data were processed, allow the consumer to correct any incorrect personal data that were processed for the purposes of such profiling and have the profiling decision reevaluated based on the corrected personal data; and (7) obtain from the controller a list of the third parties to which such controller has sold the consumer's personal data or, if such controller does not maintain a list of the third parties to which such controller has sold the consumer's personal data, a list of all third parties to which such controller has sold personal data, provided the controller shall not be required to reveal any trade secret.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 42-519 to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a consumer who the controller has actual knowledge, or wilfully disregards, is a child, the parent or legal guardian may exercise such consumer 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 guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(c) Except as otherwise provided in sections 42-515 to 42-525, inclusive, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of this section or subdivision (6) of said subsection using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (3) of subsection (a) of this section by (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to the provisions of sections 42-515 to 42-525, inclusive, or (B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of sections 42-515 to 42-525, inclusive.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

(e) A controller shall not disclose the following personal data in response to a request to exercise the consumer's rights under subdivision (1) of subsection (a) of this section, and shall instead inform the consumer or the person exercising such right on behalf of the consumer, with sufficient particularity, that the controller has collected such personal data: (1) The consumer's Social Security number; (2) the consumer's driver's license number, state identification card number or other government-issued identification number; (3) the consumer's financial account number; (4) the consumer's health insurance identification number or medical identification number; (5) the consumer's account password; (6) the consumer's security question or answer thereto; or (7) the consumer's biometric data."

(P.A. 22-15, S. 4; P.A. 25-113, S. 8.)

History: P.A. 22-15 effective July 1, 2023; P.A. 25-113 amended Subsec. (a) by adding provisions re inferences about consumer derived from personal data and profiling and adding Subdivs. (6) and (7) re processing for purposes of profiling and list of third parties to which controller has sold personal data, amended Subsec. (b) by substituting actual knowledge or wilful disregard for knowledge, added Subsec. (e) re nondisclosure of personal data in response to request to exercise certain consumer rights, and made technical and conforming changes, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-520. *(See end of section for amended version and effective date.) Controllers' duties. Sale of personal data to third parties. Notice and disclosure to consumers. Consumer opt-out. (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, 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, 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, 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.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (1) The categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to 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 electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

(e) (1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to sections 42-515 to 42-525, inclusive. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A) (i) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(I) Not unfairly disadvantage another controller;

(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 42-515 to 42-525, inclusive;

(III) Be consumer-friendly and easy to use by the average consumer;

(IV) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; and

(V) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A)

of this subdivision conflicts with the consumer's 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 shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, use, sale or sharing of the consumer's personal data.

(P.A. 22-15, S. 6; P.A. 23-56, S. 4; 23-98, S. 6; 23-204, S. 207.)

*Note: On and after July 1, 2026, this section, as amended by section 9 of public act 25-113, is to read as follows:

“Sec. 42-520. Controllers' duties. Processing and sale of personal data. Notice and disclosure to consumers. Consumer opt-out. (a) (1) A controller shall: (A) Limit the collection of personal data to what is reasonably necessary and proportionate in relation to the purposes for which such data are processed, as disclosed to the consumer; (B) unless the controller obtains the consumer's consent, not process the consumer's personal data for any material new purpose that is neither reasonably necessary to, nor compatible with, the purposes that were disclosed to the consumer, pursuant to subparagraph (A) of this subdivision, taking into account (i) the consumer's reasonable expectation regarding such personal data at the time such personal data were collected based on the purposes that were disclosed to the consumer pursuant to subparagraph (A) of this subdivision, (ii) the relationship that such new purpose bears to the purposes that were disclosed to the consumer pursuant to subparagraph (A) of this subdivision, (iii) the impact that processing such personal data for such new purpose might have on the consumer, (iv) the relationship between the consumer and the controller and the context in which the personal data were collected, and (v) the existence of additional safeguards, including, but not limited to, encryption or pseudonymization, in processing such personal data for such new purpose; (C) 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; (D) not process sensitive data concerning a consumer unless such processing is reasonably necessary in relation to the purposes for which such sensitive data are processed and without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a consumer who the controller has actual knowledge, or wilfully disregards, is a child, without processing such data in accordance with COPPA; (E) not process personal data in violation of any law of this state that prohibits unlawful discrimination against consumers, and any evidence, or lack of evidence, concerning proactive anti-bias testing or any similar proactive effort to avoid processing such data in violation of such law, including, but not limited to, any evidence or lack of evidence concerning the quality, efficacy, recency and scope of any such testing or effort, the results of such testing or effort and the response to the results of such testing or effort, shall be relevant to any claim available for a violation of such law and any defense available thereto; (F) not process personal data in violation of any federal law that prohibits unlawful discrimination against consumers; (G) 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; (H) not sell the sensitive data of a consumer without the consumer's consent; and (I) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, under circumstances where a controller has actual knowledge, or wilfully disregards, that the consumer is at least thirteen years of age but younger than eighteen 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, 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.

(2) Nothing in subdivision (1) of this subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(b) (1) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (A) The categories of personal data processed by the controller; (B) the purpose for processing personal data; (C) a description of the means, established pursuant to subsection (c) of this section, for consumers to submit requests to exercise their consumer rights pursuant to sections 42-515 to 42-525, inclusive, including, but not limited to, a description of (i) how consumers may exercise their consumer rights under subsection (a) of section 42-518, and (ii) how consumers may appeal controllers' decisions with regard to requests to exercise such rights; (D) the categories of personal data that the controller sells to third parties, if any; (E) the categories of third parties, if any, to which the controller sells personal data; (F) a clear and conspicuous disclosure of (i) any processing of personal data for purposes of targeted advertising, or (ii) any sale of personal data to a third party for purposes of targeted advertising; (G) an active electronic mail address or other online mechanism that consumers may use to contact the controller; (H) a statement disclosing whether the controller collects, uses or sells personal data for the purpose of training large language models; and (I) the most recent month and year during which the controller updated such privacy notice.

(2) A controller shall make the privacy notice required under subdivision (1) of this subsection publicly available: (A) Through a conspicuous hyperlink that includes the word “privacy” (i) on the home page of the controller's Internet web site, if the controller maintains an Internet web site, (ii) on the application store page or download page of a mobile device, if the controller maintains an application for use on a mobile device, and (iii) on the application's settings menu or in a similarly conspicuous and accessible location, if the controller maintains an application for use on a mobile device or other device used to connect to the Internet; (B) through a medium in which the controller regularly interacts with consumers, including, but not limited to, mail, if the controller does not maintain an Internet web site; (C) in each language in which the controller (i) provides any product or service that is subject to the privacy notice, or (ii) carries out any activity that is related to any product or service described in subparagraph (C)(i) of this subdivision; and (D) in a manner that is reasonably accessible to, and usable by, individuals with disabilities.

(3) Whenever a controller makes any retroactive material change to the controller's privacy notice or practices, the controller shall: (A) Notify the consumers affected by such material change with respect to any personal data to be collected after the effective date of such material change; and (B) provide a reasonable opportunity for the consumers described in subparagraph (A) of this subdivision to withdraw consent to any further and materially different collection, processing or transfer of previously collected personal data following such material change. The controller shall take all reasonable electronic measures to provide such notice to such affected consumers, taking into account the technology available to the controller and the nature of the controller's relationship with such affected consumers.

(4) Nothing in this subsection shall be construed to require a controller to provide a privacy notice that is specific to this state if the controller provides a generally applicable privacy notice that satisfies the requirements established in this subsection.

(c) (1) A controller shall establish one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to sections 42-515 to 42-525, inclusive. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A) (i) Providing a clear and conspicuous hyperlink on the controller's Internet web site to an Internet web page that enables the consumer, or an agent of the consumer, to opt out of the processing of the consumer's personal data for purposes of targeted advertising, or any sale of the consumer's personal data; and

(ii) Allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(I) Not unfairly disadvantage another controller;

(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 42-515 to 42-525, inclusive;

(III) Be consumer-friendly and easy to use by the average consumer;

(IV) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; and

(V) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this subdivision conflicts with the consumer's 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 shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subdivision (2) of subsection (a) of this section for the retention, use, sale or sharing of the consumer's personal data.”

(P.A. 22-15, S. 6; P.A. 23-56, S. 4; 23-98, S. 6; 23-204, S. 207; P.A. 25-113, S. 9.)

History: P.A. 22-15 effective July 1, 2023; P.A. 23-56 amended Subsec. (a)(7) by substituting “or wilfully disregards” for “and wilfully disregards”, effective July 1, 2023; P.A. 23-98 made identical changes as P.A. 23-56, effective July 1, 2023; P.A. 23-204 changed effective date of P.A. 23-56, S. 4, from July 1, 2023, to October 1, 2023, effective June 12, 2023; P.A. 25-113 substantially revised section including Subsec. (a) by redesignating existing provisions as Subdiv. (1), replacing “adequate, relevant and reasonably necessary” with “reasonably necessary and proportionate” and enumerating factors to be considered, replacing “known” with “actual knowledge, or wilfully disregards” re whether consumer is a child, adding provisions re proactive anti-bias training and prohibiting sale of sensitive data without consumer consent and replacing “sixteen” with “eighteen” before “years of age”, redesignating existing Subsec. (b) as Subsec. (a)(2), Subsec. (c) by redesignating existing provisions as Subsec. (b)(1), adding Subdiv. (1)(C), (F), (H) and (I) re description of means to submit request to exercise consumer rights, clear and conspicuous disclosure of processing or sale of personal data for purposes of targeted advertising, statement disclosing collection, use or sale of personal data to train large language model and disclosure re most recent month and year during which controller updated privacy notice, adding new Subdivs. (2) to (4) re means by which controller makes privacy notice publicly available, controller's duties in response to making retroactive material change to controller's privacy notice or practices and generally applicable privacy notice, deleting former Subsec. (d) re controller sale of personal data to third party or processing personal data for targeted advertising, redesignating existing Subsec. (e) as Subsec. (c) and deleting provision therein re description in privacy notice of means available for consumer to request to exercise consumer rights, making technical and conforming changes, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-521. *(See end of section for amended version and effective date.) Processors' duties. Contracts between controllers and processors. (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 42-515 to 42-525, inclusive. Such assistance shall include: (1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests; (2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b, of the system of the processor, in order to meet the controller's obligations; and (3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 42-515 to 42-525, inclusive; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 42-515 to 42-525, inclusive, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(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 42-515 to 42-525, inclusive.

(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 42-525.

(P.A. 22-15, S. 7.)

*Note: On and after July 1, 2026, this section, as amended by section 10 of public act 25-113, is to read as follows:

“Sec. 42-521. Processors' duties. Contracts between controllers and processors. (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 42-515 to 42-525, inclusive. Such assistance shall include: (1) Taking into account the nature of processing and insofar as is possible, to fulfill the controller's obligation to respond to consumers' requests to exercise their rights under section 42-518; (2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b, of the system of the processor, in order to meet the controller's obligations; and (3) providing necessary information to enable the controller to conduct and document data protection assessments and impact assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 42-515 to 42-525, inclusive; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 42-515 to 42-525, inclusive, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(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 42-515 to 42-525, inclusive.

(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 are 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 42-525.”

(P.A. 22-15, S. 7; P.A. 25-113, S. 10.)

History: P.A. 22-15 effective July 1, 2023; P.A. 25-113 substantially revised Subsec. (a)(1) including by deleting provision re information available to processor by appropriate technical and organizational measures, substituting “possible” for “reasonably practicable” and adding provision re consumer request to exercise rights under Sec. 42-518, amended Subsec. (a)(3) by adding reference to impact assessments, and made a technical change in Subsec. (d), effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-522. *(See end of section for amended version and effective date.) Controllers' data protection assessments. Disclosure to Attorney General. (a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (1) The processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in sections 42-515 to 42-525, inclusive. Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

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

(e) 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.

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

(P.A. 22-15, S. 8.)

*Note: On and after July 1, 2026, this section, as amended by section 11 of public act 25-113, is to read as follows:

“Sec. 42-522. Controllers' data protection and impact assessments. Disclosure to Attorney General. (a) For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (1) The processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data.

(b) (1) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.

(2) Each data protection assessment conducted pursuant to subdivision (1) of this subsection shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into each such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) Each controller that engages in any profiling for the purposes of making a decision that produces any legal or similarly significant effect concerning a consumer shall conduct an impact assessment for such profiling. Such impact assessment shall include, to the extent reasonably known by or available to the controller, as applicable: (1) A statement by the controller disclosing the purpose, intended use cases and deployment context of, and benefits afforded by, such profiling; (2) an analysis of whether such profiling poses any known or reasonably foreseeable heightened risk of harm to a consumer, and, if so, (A) the nature of such heightened risk of harm to a consumer, and (B) the steps that have been taken to mitigate such heightened risk of harm to a consumer; (3) a description of (A) the main categories of personal data processed as inputs for the purposes of such profiling, and (B) the outputs such profiling produces; (4) an overview of the main categories of personal data the controller used to customize such profiling, if the controller used data to customize such profiling; (5) any metrics used to evaluate the performance and known limitations of such profiling; (6) a description of any transparency measures taken concerning such profiling, including, but not limited to, any measures taken to disclose to consumers that such controller is engaged in such profiling while such controller is engaged in such profiling; and (7) a description of the post-deployment monitoring and user safeguards provided concerning such profiling, including, but not limited to, the oversight, use and learning processes established by the controller to address issues arising from such profiling.

(d) The Attorney General may require that a controller disclose any data protection assessment or impact assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment or impact assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment or impact assessment for compliance with the responsibilities set forth in sections 42-515 to 42-525, inclusive. Data protection assessments and impact assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200. To the extent any information contained in a data protection assessment or impact assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

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

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

(g) (1) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

(2) Impact assessment requirements shall apply to processing activities created or generated on or after August 1, 2026, and are not retroactive."

(P.A. 22-15, S. 8; P.A. 25-113, S. 11.)

History: P.A. 22-15 effective July 1, 2023; P.A. 25-113 redesignated as new Subsec. (a) existing provisions re processing that presents heightened risk of harm to consumer, redesignated existing Subsecs. (a) to (f) as Subsecs. (b)(1) and (2) and (d) to (g)(1), added new Subsec. (c) re impact assessments, added provisions re impact assessments in redesignated Subsecs. (d) to (f), added Subsec. (g)(2) re prospective application of impact assessment requirements, and made technical and conforming changes, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-524. *(See end of section for amended versions of subsections (a) to (d) and effective date.) Construction of controllers', consumer health date controllers' and processors' duties. *(a) Nothing in sections 42-515 to 42-526, inclusive, shall be construed to restrict a controller's, 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, 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 42-526, inclusive; 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, processors or consumer health data controllers under sections 42-515 to 42-526, inclusive, shall not restrict a controller's, 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, processors or consumer health data controllers under sections 42-515 to 42-526, inclusive, shall not apply where compliance by the controller, 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 42-526, inclusive, shall be construed to prevent a controller, 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, processor or consumer health data controller that discloses personal data to a processor or third-party controller in accordance with sections 42-515 to 42-526, inclusive, 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, processor or consumer health data controller disclosed such personal data, the disclosing controller, 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, processor or consumer health data controller in compliance with sections 42-515 to 42-526, inclusive, is likewise not in violation of said sections for the transgressions of the controller, 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 42-526, inclusive, shall be construed to: (1) Impose any obligation on a controller, 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.

(P.A. 22-15, S. 10; P.A. 23-56, S. 5; 23-204, S. 207.)

*Note: On and after July 1, 2026, subsections (a) to (d) of this section, as amended by section 12 of public act 25-113, are to read as follows:

“(a) Nothing in sections 42-515 to 42-526, inclusive, shall be construed to restrict a controller's, 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, 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 42-526, inclusive; 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 are 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, processors or consumer health data controllers under sections 42-515 to 42-526, inclusive, shall not restrict a controller's, 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; (4) process personal data for

the purposes of profiling in furtherance of any automated decision that may produce any legal or similarly significant effect concerning a consumer, provided such personal data are (A) processed only to the extent necessary to detect or correct any bias that may result from processing such data for such purposes, such bias cannot effectively be detected or corrected without processing such data and such data are deleted once such processing has been completed, (B) processed subject to appropriate safeguards to protect the rights of consumers secured by the Constitution or laws of this state or of the United States, (C) subject to technical restrictions concerning the reuse of such data and industry-standard security and privacy measures, including, but not limited to, pseudonymization, (D) subject to measures to ensure that such data are secure, protected and subject to suitable safeguards, including, but not limited to, strict controls concerning, and documentation of, access to such data, to avoid misuse and ensure that only authorized persons may access such data while preserving the confidentiality of such data, and (E) not transmitted, transferred or otherwise accessed by any third party; (5) 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; or (6) perform internal operations in accordance with the internal operations exception established in COPPA if the controller, processor or consumer health data controller is processing data in accordance with such exception.

(c) The obligations imposed on controllers, processors or consumer health data controllers under sections 42-515 to 42-526, inclusive, shall not apply where compliance by the controller, 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 42-526, inclusive, shall be construed to prevent a controller, 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, processor or consumer health data controller that discloses personal data to a processor or third-party controller in accordance with sections 42-515 to 42-526, inclusive, 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, processor or consumer health data controller disclosed such personal data, the disclosing controller, 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, processor or consumer health data controller in compliance with sections 42-515 to 42-526, inclusive, is likewise not in violation of said sections for the transgressions of the controller, processor or consumer health data controller from which such third-party controller or processor receives such personal data."

(P.A. 22-15, S. 10; P.A. 23-56, S. 5; 23-204, S. 207; P.A. 25-113, S. 12.)

History: P.A. 22-15 effective July 1, 2023; P.A. 23-56 amended Subsecs. (a) to (e) by adding references to consumer health data controllers and Sec. 42-526, amended Subsecs. (f) to (h) by adding references to consumer health data controllers, and made technical and conforming changes throughout, effective July 1, 2023; P.A. 23-204 changed effective date of P.A. 23-56, S. 5, from July 1, 2023, to October 1, 2023, effective June 12, 2023; P.A. 25-113 amended Subsec. (b) by adding new Subdiv. (4) re processing personal data for purposes of profiling in furtherance of automated decision that may produce legal or similarly significant effect concerning consumer, redesignating existing Subdiv. (4) as Subdiv. (5) and adding Subdiv. (6) re internal operations exception established in COPPA, and made a technical change in Subsec. (a), effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

PART II

SOCIAL MEDIA PLATFORMS, ONLINE SERVICES, PRODUCTS OR FEATURES AND MINORS

(A)

SOCIAL MEDIA PLATFORMS AND MINORS

Sec. 42-528. *(See end of section for amended versions of subsections (a) and (b) and effective date.) Social media platforms and minors. Request to unpublish or delete minor's account. Enforcement. Penalty. *(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;

(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;

(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. 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 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.

(P.A. 23-56, S. 7.)

*Note: On and after July 1, 2026, subsections (a) and (b) of this section, as amended by section 13 of public act 25-113, are to read as follows:

“(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;

(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;

(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. 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.

(4) No social media platform shall require a minor's parent or legal guardian to create a social media platform account to submit a request pursuant to this subsection. A social media platform may require a minor's parent or legal guardian to use an existing social media platform account to submit such a request, provided such parent or legal guardian has access to the existing social media platform account.”

(P.A. 23-56, S. 7; P.A. 25-113, S. 13.)

History: P.A. 23-56 effective July 1, 2024; P.A. 25-113 added Subsec. (b)(4) prohibiting requirement re creation of social media platform account by parent or legal guardian, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

(B)

ONLINE SERVICES, PRODUCTS OR FEATURES AND MINORS

Sec. 42-529. *(See end of section for amended version and effective date.) Definitions. For the purposes of this section and sections 42-529a to 42-529e, inclusive:

(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;

(3) “Consumer” has the same meaning as provided in section 42-515;

(4) “Controller” has the same meaning as provided in section 42-515;

(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;

(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;

(10) “Personal data” has the same meaning as provided in section 42-515;

(11) “Precise geolocation data” has the same meaning as provided in section 42-515;

(12) “Process” and “processing” have the same meaning as provided in section 42-515;

(13) “Processor” has the same meaning as provided in section 42-515;

(14) “Profiling” has the same meaning as provided in section 42-515;

(15) “Protected health information” has the same meaning as provided in section 42-515;

(16) “Sale of personal data” has the same meaning as provided in section 42-515;

(17) “Targeted advertising” has the same meaning as provided in section 42-515; and

(18) “Third party” has the same meaning as provided in section 42-515.

(P.A. 23-56, S. 8.)

*Note: On and after July 1, 2026, this section, as amended by section 14 of public act 25-113, is to read as follows:

“Sec. 42-529. Definitions. For the purposes of this section and sections 42-529a to 42-529e, inclusive:

(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;

(3) “Consumer” has the same meaning as provided in section 42-515;

(4) “Controller” has the same meaning as provided in section 42-515;

(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 material financial, physical or reputational injury to minors, (C) any material 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, (D) any physical violence against minors, (E) any material harassment of minors on any online service, product or feature, which harassment is severe, pervasive or objectively offensive to a reasonable person, or (F) any sexual abuse or sexual exploitation of minors;

(6) “HIPAA” has the same meaning as provided in section 42-515;

(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;

(10) “Personal data” has the same meaning as provided in section 42-515;

(11) “Precise geolocation data” has the same meaning as provided in section 42-515;

(12) “Process” and “processing” have the same meaning as provided in section 42-515;

(13) “Processor” has the same meaning as provided in section 42-515;

(14) “Profiling” has the same meaning as provided in section 42-515;

(15) “Protected health information” has the same meaning as provided in section 42-515;

(16) “Sale of personal data” has the same meaning as provided in section 42-515;

(17) “Targeted advertising” has the same meaning as provided in section 42-515; and

(18) “Third party” has the same meaning as provided in section 42-515.”

(P.A. 23-56, S. 8; P.A. 25-113, S. 14.)

History: P.A. 23-56 effective October 1, 2024; P.A. 25-113 amended Subdiv. (5) by redefining “heightened risk of harm to minors”, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-529a. *(See end of section for amended version and effective date.) Controllers' duties. Consumer consent. (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 42-529e, 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 42-529b 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.

(P.A. 23-56, S. 9.)

*Note: On and after July 1, 2026, this section, as amended by section 15 of public act 25-113, is to read as follows:

“Sec. 42-529a. Controllers' duties. Consumer consent. (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 42-529e, 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 42-529b concerning data protection assessments and impact assessments.

(b) (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 process any minor's personal data: (A) For the purposes of (i) targeted advertising, or (ii) any sale of personal data; (B) unless such processing is reasonably necessary to provide such online service, product or feature; (C) 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) other than what is reasonably necessary for, and compatible with, the processing purpose described in subparagraph (C)(i) of this subdivision; or (D) for longer than is reasonably necessary to provide 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) 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 are strictly necessary for the controller to provide such online service, product or feature and, if such data are 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) (A) Subject to the consent requirement established in subparagraph (B) of this subdivision, no controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall process any minor's personal data for purposes of profiling in furtherance of any 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 service, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care service or access to any essential good or service, unless such processing is reasonably necessary to provide such online service, product or feature.

(B) No controller shall engage in the activities described in subparagraph (A) of this subdivision 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 subparagraph.

(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; (B) except as provided in subdivision (2) of this subsection, offer any direct messaging apparatus for use by minors unless (i) such controller provides readily accessible and easy-to-use safeguards to enable any minor, or any minor's parent or legal guardian, to prevent any adult from sending any unsolicited communication to such minor unless such minor and adult are already connected on such online service, product or feature, and (ii) the safeguards required under subparagraph (B)(i) of this subdivision, as a default setting, prevent any adult from sending any unsolicited communication to any minor unless such minor and adult are already connected on such online service, product or feature; or (C) except as provided in subdivision (3) of this subsection, use any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature.

(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.

(3) The provisions of subparagraph (C) of subdivision (1) of this subsection 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."

(P.A. 23-56, S. 9; P.A. 25-113, S. 15.)

History: P.A. 23-56 effective October 1, 2024; P.A. 25-113 amended Subsec. (a) by adding provision re impact assessments, substantially amended Subsec. (b) including by deleting provisions in Subdivs. (1) and (2) re consent requirement established in redesignated Subdiv. (3)(B), deleting provisions in Subdiv. (1) re profiling in furtherance of fully automated decision that produces legal or similarly significant effect concerning certain services and system design feature used to significantly increase, sustain or extend use by minor, replacing "is reasonably" with "are strictly" before "necessary" in Subdiv. (2), adding Subdiv. (3)(A) re exception for processing reasonably necessary to provide online service, product or feature and redesignating existing Subdiv. (3) as Subdiv. (3)(B), substantially amended Subsec. (c) including by adding provisions in Subdiv. (1) re provision of safeguards to minor, parent or legal guardian and adding Subdiv. (3) re educational entity, and made technical and conforming changes, effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-529b. *(See end of section for amended version and effective date.) Controllers' data protections assessments. Review, record keeping, confidentiality and disclosure. Risk mitigation plan. (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; 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. 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.

(P.A. 23-56, S. 10.)

*Note: On and after July 1, 2026, this section, as amended by section 16 of public act 25-113, is to read as follows:

"Sec. 42-529b. Controllers' data protection and impact assessments. Review, record keeping, confidentiality and disclosure. Plans. (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 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; 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 offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall, if such online service, product or feature engages in any profiling based on such consumers' personal data, conduct an impact assessment for such online service, product or feature. Such impact assessment shall include, to the extent reasonably known by or available to the controller, as applicable: (1) A statement by the controller disclosing the purpose, intended use cases and deployment context of, and benefits afforded by, such online service, product or feature, if such online service, product or feature engages in any profiling for the purpose of making decisions that produce legal or similarly significant effects concerning such consumers; (2) an analysis of whether such profiling poses any reasonably foreseeable heightened risk of harm to minors and, if so, (A) the nature of such heightened risk of harm to minors, and (B) the steps that have been taken to mitigate such heightened risk of harm to minors; (3) a description of (A) the categories of personal data such online service, product or feature processes as inputs for the purposes of such profiling, and (B) the outputs such online service, product or feature produces for the purposes of such profiling; (4) an overview of the categories of personal data the controller used to customize such online service, product or feature for the purposes of such profiling, if the controller used data to customize such online service, product or feature for the purposes of such profiling; (5) a description of any transparency measures taken concerning such online service, product or feature with respect to such profiling, including, but not limited to, any measures taken to disclose to consumers that such online service, product or feature is being used for such profiling while such online service, product or feature is being used for such profiling; and (6) a description of the post-deployment monitoring and user safeguards provided concerning such online service, product or feature for the purposes of such profiling, including, but not limited to, the oversight, use and learning processes established by the controller to address issues arising from deployment of such online service, product or feature for the purposes of such profiling.

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

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

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

(f) If any controller conducts a data protection assessment pursuant to subsection (a) of this section, or an impact assessment pursuant to subsection (b) 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. The Attorney General may require a controller to disclose to the Attorney General a plan established pursuant to this subsection if the plan is relevant to an investigation conducted by the Attorney General. The controller shall disclose such plan to the Attorney General not later than ninety days after the Attorney General notifies the controller, in a form and manner prescribed by the Attorney General, that the Attorney General requires the controller to disclose such plan to the Attorney General.

(g) Data protection assessments, impact assessments and harm mitigation or elimination plans shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200. To the extent any information contained in a data protection assessment, impact assessment or harm mitigation or elimination plan 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."

(P.A. 23-56, S. 10; P.A. 25-113, S. 16.)

History: P.A. 23-56 effective October 1, 2024; P.A. 25-113 added new Subsec. (b) re profiling and impact assessments, redesignated existing Subsecs. (b) to (f) as Subsecs. (c) to (g), amended redesignated Subsecs. (c) and (d) by adding provisions re profiling and impact assessments, amended redesignated Subsec. (e) by adding provisions re impact assessments, amended redesignated Subsec. (f) by adding provisions re impact assessments and plan disclosure to Attorney General, amended redesignated Subsec. (g) by adding provisions re impact assessments and plans and made a technical change in Subsec. (a), effective July 1, 2026.

Sec. 42-529c. *(See end of section for amended version of subsection (a) and effective date.) Processors' duties. Contracts between controllers and processors. *(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 42-529 to 42-529e, inclusive, 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.

(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 42-529 to 42-529e, inclusive.

(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 42-529e.

(P.A. 23-56, S. 11.)

*Note: On and after July 1, 2026, subsection (a) of this section, as amended by section 17 of public act 25-113, is to read as follows:

“(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 42-529 to 42-529e, inclusive, 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 and impact assessments pursuant to section 42-529b.”

(P.A. 23-56, S. 11; P.A. 25-113, S. 17.)

History: P.A. 23-56 effective October 1, 2024; P.A. 25-113 amended Subsec. (a)(2) by adding provision re impact assessments and reference to Sec. 42-529b, effective July 1, 2026.

Sec. 42-529d. *(See end of section for amended version of subsection (d) and effective date.) Exemptions. (a) The provisions of sections 42-529 to 42-529c, inclusive, and section 42-529e 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 42-529 to 42-529c, inclusive, and section 42-529e: (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 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 42-529 to 42-529c, inclusive, and section 42-529e 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 42-529 to 42-529c, inclusive, or section 42-529e 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 42-529 to 42-529c, inclusive, or section 42-529e; 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 42-529 to 42-529c, inclusive, or section 42-529e 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 42-529 to 42-529c, inclusive, or section 42-529e 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 42-529 to 42-529c, inclusive, or section 42-529e 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; 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.

(P.A. 23-56, S. 12.)

*Note: On and after July 1, 2026, subsection (d) of this section, as amended by section 18 of public act 25-113, is to read as follows:

"(d) No obligation imposed on a controller or processor under any provision of sections 42-529 to 42-529c, inclusive, or section 42-529e 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; (4) process personal data for the purposes of profiling in furtherance of any automated decision that may produce any legal or similarly significant effect concerning a consumer, provided such personal data are (A) processed only to the extent necessary to detect or correct any bias that may result from processing such personal data for such purposes, such bias cannot effectively be detected or corrected without processing such personal data and such personal data are deleted once such processing has been completed, (B) processed subject to appropriate safeguards to protect the rights of consumers secured by the Constitution or laws of this state or of the United States, (C) subject to technical restrictions concerning the reuse of such personal data and industry-standard security and privacy measures, including, but not limited to, pseudonymization, (D) subject to measures to ensure that such personal data are secure, protected and subject to suitable safeguards, including, but not limited to, strict controls concerning, and documentation of, access to such personal data, to avoid misuse and ensure that only authorized persons may access such personal data while preserving the confidentiality of such personal data, and (E) not transmitted, transferred or otherwise accessed by any third party; or (5) perform solely 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."

(P.A. 23-56, S. 12; P.A. 25-113, S. 18.)

History: P.A. 23-56 effective October 1, 2024; P.A. 25-113 amended Subsec. (d) by adding new Subdiv. (4) re processing personal data for purposes of profiling, redesignating existing Subdiv. (4) as Subdiv. (5) and adding "solely" before "internal operations" in redesignated Subdiv. (5), effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

PART III

SOCIAL MEDIA PLATFORMS

Sec. 42-530. (Note: This section is effective July 1, 2026.) Social media platform to incorporate online safety center and establish cyberbullying policy. (a) As used in this section:

(1) "Consumer" means an individual who is a resident of this state and a user of a social media platform;

(2) "Cyberbullying" means any act, carried out on a social media platform, that (A) is reasonably likely to (i) cause physical or emotional harm to a consumer, or (ii) place a consumer in fear of physical or emotional harm, or (B) infringes on any right afforded to a consumer under the laws of this state or federal law;

(3) "Mental health services" has the same meaning as provided in section 19a-498c;

(4) “Owner” means the person who owns a social media platform;

(5) “Person” means an individual, association, corporation, limited liability company, partnership, trust or other legal entity; and

(6) “Social media platform” has the same meaning as provided in section 42-528.

(b) Not later than October 1, 2026, each owner of a social media platform shall incorporate an online safety center into the social media platform. Each online safety center shall, at a minimum, provide the consumers who use such social media platform with:

(1) Resources for the purposes of (A) preventing cyberbullying on such social media platform, and (B) enabling any consumer to identify any means available to such consumer to obtain mental health services, including, but not limited to, an Internet web site address or telephone number where such consumer may obtain mental health services for the treatment of an anxiety disorder or the prevention of suicide;

(2) Access to online behavioral health educational resources;

(3) An explanation of such social media platform's mechanism for reporting harmful or unwanted behavior, including, but not limited to, cyberbullying, on such social media platform; and

(4) Educational information concerning the impact that social media platforms have on users' mental health.

(c) Not later than October 1, 2026, each owner of a social media platform shall establish a cyberbullying policy for the social media platform. Such policy shall, at a minimum, set forth the manner in which such owner handles reports of cyberbullying on such social media platform.

(P.A. 25-113, S. 4.)

History: P.A. 25-113 effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

PART IV

CONNECTED DEVICES AND SERVICES

Sec. 42-531. (Note: This section is effective July 1, 2026.) Connected devices. Requirements. Exceptions. Unfair or deceptive trade practice. (a) For the purposes of this section:

(1) “Connected device” means an Internet-connected home appliance, television or toy that includes a camera or microphone;

(2) “Connected device manufacturer” means a person doing business in this state who manufactures a connected device;

(3) “Initial consumer” means an individual who is (A) a resident of this state, and (B) with respect to any connected device, the first individual to lease, purchase or assume ownership of such connected device;

(4) “Person” means an individual, association, corporation, limited liability company, partnership, trust or other legal entity;

(5) “Personally identifying information” has the same meaning as provided in section 42-284;

(6) “Provider” means (A) a connected device manufacturer, and (B) any person who (i) enters into a contract with a connected device manufacturer, and (ii) receives access to (I) any camera or microphone included in a connected device manufactured by the connected device manufacturer, (II) any image or video collected, recorded, stored, analyzed, interpreted or transmitted by way of any camera included in any connected device manufactured by the connected device manufacturer, or (III) any spoken word or other sound collected, recorded, stored, analyzed, interpreted or transmitted by way of any microphone included in any connected device manufactured by the connected device manufacturer; and

(7) “Toy” means a product that a manufacturer designs, or intends to be used, for amusement or play.

(b) No provider shall allow any person to activate any connected device unless the provider:

(1) Prominently displays to the initial consumer or any person whom the initial consumer designates to first install or set up the connected device, at the time that such initial consumer or person first installs or sets up such connected device:

(A) A disclaimer in the following form:

“This device transmits audio and/or video back to the manufacturer and/or a third party and which may be recorded.”; and

(B) A statement disclosing (i) that such connected device includes a camera or microphone, (ii) that the camera or microphone included in such connected device will be enabled or turned on, (iii) that such connected device might record such initial consumer, (iv) that the connected device manufacturer of such connected device or another provider might retain recordings of such initial consumer, (v) which command or action will activate or enable operation of the camera or microphone included in such connected device, (vi) the categories of images, videos or sounds that (I) the camera or microphone included in such connected device will look for, listen for or record, or (II) might be disclosed to any person other than such initial consumer, (vii) the categories of persons described in subparagraph (B)(vi)(II) of this subdivision, and (viii) that such initial consumer shall not be discriminated against if such initial consumer or person declines to activate a camera or microphone included in the connected device unless (I) such connected device is provided to such initial consumer as a condition of employment, or (II) declining to activate such camera or microphone would render such connected device useless; and

(2) Provides to the initial consumer or any person whom the initial consumer designates to first install or set up the connected device, at the time that such initial consumer or person first installs or sets up such connected device, the ability to decline to activate a camera or microphone included in the connected device, unless declining to activate the camera or microphone would render such connected device useless.

(c) Each provider shall implement and maintain reasonable security measures to protect any personally identifying information collected through a camera or microphone included in a connected device from any unauthorized access, acquisition, destruction, disclosure, modification or use thereof.

(d) No provider shall use or sell any recording collected through operation of a camera or microphone included in a connected device for the purposes of targeted advertising, as defined in section 42-515, unless the initial consumer opts in to such use or sale for such purposes.

(e) No person shall compel any provider to build specific features for the purpose of allowing a law enforcement agency or officer to monitor communications through a camera or microphone included in a connected device.

(f) Nothing in this section shall be construed to:

(1) Impose any liability on a provider for any functionality provided by an application that an initial consumer (A) downloads and installs, or (B) chooses to use on a network of remote servers hosted on the Internet to store, manage and process data;

(2) Authorize disclosure of any recording retained by a provider to another person, including, but not limited to, a law enforcement agency or officer, unless such disclosure is authorized by other applicable law or pursuant to an order issued by a court of competent jurisdiction; or

(3) Modify, limit or supersede the operation of any other provision of the general statutes concerning privacy or security.

(g) Any violation of subsections (b) to (d), inclusive, of this section shall be deemed an unfair or deceptive trade practice under subsection (a) of section 42-110b.

(P.A. 25-44, S. 2.)

History: P.A. 25-44 effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 42-531a. (Note: This section is effective July 1, 2026.) Connected vehicle services. Requirements re survivors and covered providers. Immunity from civil liability. (a) As used in this section:

(1) “Abuser” means an individual who (A) is identified by a survivor pursuant to subsection (b) of this section, and (B) has committed, or allegedly committed, a covered act against the survivor making the connected vehicle services request;

(2) “Account holder” means an individual who is (A) a party to a contract with a covered provider that involves a connected vehicle service, or (B) a subscriber, customer or registered user of a connected vehicle service;

(3) “Connected vehicle service” means any capability provided by or on behalf of a motor vehicle manufacturer that enables a person to remotely obtain data from, or send commands to, a covered vehicle, including, but not limited to, any such capability provided by way of a software application that is designed to be operated on a mobile device;

(4) “Connected vehicle service request” means a request by a survivor to terminate or disable an abuser's access to a connected vehicle service;

(5) “Covered act” means conduct that constitutes (A) a crime described in Section 40002(a) of the Violence Against Women Act of 1994, 34 USC 12291(a), as amended from time to time, (B) an act or practice described in 22 USC 7102(11) or (12), as amended from time to time, or (C) a crime, act or practice that is (i) similar to a crime, act or practice described in subparagraph (A) or (B) of this subdivision, and (ii) prohibited under federal, state or tribal law;

(6) “Covered connected vehicle services account” means an account or other means by which a person enrolls in, or obtains access to, a connected vehicle service;

(7) “Covered provider” means a motor vehicle manufacturer, or an entity acting on behalf of a motor vehicle manufacturer, that provides a connected vehicle service;

(8) “Covered vehicle” means a motor vehicle that is (A) the subject of a connected vehicle request, and (B) identified by a survivor pursuant to subsection (b) of this section;

(9) “Emergency situation” means a situation that, if allowed to continue, poses an imminent risk of death or serious bodily harm;

(10) “In-vehicle interface” means a feature or mechanism installed in a motor vehicle that allows an individual within the motor vehicle to terminate or disable connected vehicle services;

(11) “Person” means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity; and

(12) “Survivor” means an individual (A) who is eighteen years of age or older, and (B) against whom a covered act has been committed or allegedly committed.

(b) A survivor may submit a connected vehicle service request to a covered provider pursuant to this subsection. Each connected vehicle service request submitted pursuant to this subsection shall, at a minimum, include (1) the vehicle identification number of the covered vehicle, (2) the name of the abuser, and (3) (A) proof that the survivor is the sole owner of the covered vehicle, (B) if the survivor is not the sole owner of the covered vehicle, proof that the survivor is legally entitled to exclusive possession of the covered vehicle, which proof may take the form of a court order awarding exclusive possession of the covered vehicle to the survivor, or (C) if the abuser owns the covered vehicle, in whole or in part, a dissolution of marriage decree, restraining order or temporary restraining order (i) naming the abuser, and (ii) (I) granting exclusive possession of the covered vehicle to the survivor, or (II) restricting the abuser's use of a connected vehicle service against the survivor.

(c) (1) Not later than two business days after a survivor submits a connected vehicle service request to a covered provider pursuant to subsection (b) of this section, the covered provider shall take one or more of the following actions requested by the survivor in the connected vehicle service request, regardless of whether the abuser identified in the connected vehicle service request is an account holder: (A) Terminate or disable the covered connected vehicle services account associated with such abuser; (B) (i) terminate or disable the covered connected vehicle services account associated with the covered vehicle, including, but not limited to, by resetting or deleting any data or wireless connection with respect to the covered vehicle, and (ii) provide instructions to the survivor on how to reestablish a covered connected vehicle services account; (C) (i) terminate or disable covered connected vehicle services for the covered vehicle, including, but not limited to, by resetting or deleting any data or wireless connection with respect to the covered vehicle, and (ii) provide instructions to the survivor on how to reestablish connected vehicle services; or (D) if the motor vehicle has an in-vehicle interface, provide information to the survivor concerning (i) the availability of the in-vehicle interface, and (ii) how to terminate or disable connected vehicle services using the in-vehicle interface.

(2) After the covered provider has taken action pursuant to subdivision (1) of this subsection, the covered provider shall deny any request made by the abuser to obtain any data that (A) were generated by the connected vehicle service after the abuser's access to such connected vehicle service was terminated or disabled in response to the connected vehicle service request, and (B) are maintained by the covered provider.

(3) The covered provider shall not refuse to take action pursuant to subdivision (1) of this subsection on the basis that any requirement, other than a requirement established in subsection (b) of this section, has not been satisfied, including, but not limited to, any requirement that provides for (A) payment of any fee, penalty or other charge, (B) maintaining or extending the term of the covered connected vehicle services account, (C) obtaining approval from any account holder other than the survivor, or (D) increasing the rate charged for the connected vehicle service.

(4) (A) If the covered provider intends to provide any formal notice to the abuser regarding any action set forth in subdivision (1) of this subsection, the covered provider shall first notify the survivor of the date on which the covered provider intends to provide such notice to the abuser.

(B) The covered provider shall take reasonable steps to ensure that the covered provider only provides formal notice to the abuser, pursuant to subparagraph (A) of this subdivision, (i) at least three days after the covered provider notified the survivor pursuant to subparagraph (A) of this subdivision, and (ii) after the covered provider has terminated or disabled the abuser's access to the connected vehicle service.

(5) (A) The covered provider shall not be required to take any action pursuant to subdivision (1) of this subsection if the covered provider cannot operationally or technically effectuate such action.

(B) If the covered provider cannot operationally or technically effectuate any action as set forth in subparagraph (A) of this subdivision, the covered provider shall promptly notify the survivor who submitted the connected vehicle service request that the covered provider cannot operationally or technically effectuate such action, which notice shall, at a minimum, disclose whether the covered provider's inability to operationally or technically effectuate such action can be remedied and, if so, any steps the survivor can take to assist the covered provider in remedying such inability.

(d) (1) The covered provider and each officer, director, employee, vendor or agent of the covered provider shall treat all information submitted by the survivor under subsection (b) of this section as confidential, and shall securely dispose of such information not later than ninety days after the survivor submitted such information.

(2) The covered provider shall not disclose any information submitted by the survivor under subsection (b) of this section to a third party unless (A) the covered provider has obtained affirmative consent from the survivor to disclose such information to the third party, or (B) disclosing such information to the third party is necessary to effectuate the connected vehicle service request.

(3) Nothing in subdivision (1) of this subsection shall be construed to prohibit the covered provider from maintaining, for longer than the period specified in subdivision (1) of this subsection, a record that verifies that the survivor fulfilled the conditions of the connected vehicle service request as set forth in subsection (b) of this section, provided such record is limited to what is reasonably necessary and proportionate to verify that the survivor fulfilled such conditions.

(e) The survivor shall take reasonable steps to notify the covered provider of any change in the ownership or possession of the covered vehicle that materially affects the need for the covered provider to take action pursuant to subdivision (1) of subsection (c) of this section.

(f) The requirements established in this section shall not prohibit or prevent a covered provider from terminating or disabling an abuser's access to a connected vehicle service in an emergency situation after receiving a connected vehicle service request.

(g) Each covered provider shall publicly post, on such covered provider's Internet web site, a statement describing how a survivor may submit a connected vehicle service request to such covered provider.

(h) Each covered provider and each officer, director, employee, vendor or agent of a covered provider shall be immune from any civil liability which might otherwise arise from any act or omission committed by such covered provider, officer, director, employee, vendor or agent pursuant to subsections (a) to (g), inclusive, of this section, provided such act or omission was committed in compliance with the provisions of said subsections.

(P.A. 25-113, S. 19.)

History: P.A. 25-113 effective July 1, 2026.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)