



General Assembly

Amendment

January Session, 2025

LCO No. 8182



Offered by:

SEN. MARONEY, 14th Dist.

REP. LEMAR, 96th Dist.

REP. TURCO, 27th Dist.

To: Subst. Senate Bill No. 1356

File No. 609

Cal. No. 334

**"AN ACT CONCERNING DATA PRIVACY, ONLINE MONITORING,
SOCIAL MEDIA, DATA BROKERS AND CONNECTED VEHICLE
SERVICES."**

1 Strike everything after the enacting clause and substitute the
2 following in lieu thereof:

3 "Section 1. (NEW) (*Effective October 1, 2025*) (a) As used in this section:

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

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

11 (3) "Mental health services" has the same meaning as provided in

12 section 19a-498c of the general statutes;

13 (4) "Owner" means the person who owns a social media platform;

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

16 (6) "Social media platform" has the same meaning as provided in
17 section 42-528 of the general statutes, as amended by this act.

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

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

28 (2) Access to online behavioral health educational resources;

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

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

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

39 Sec. 2. Section 42-515 of the general statutes is repealed and the

40 following is substituted in lieu thereof (*Effective October 1, 2025*):

41 As used in this section and sections 42-516 to 42-526, inclusive, as
42 amended by this act, unless the context otherwise requires:

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

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

54 (3) "Authenticate" means to use reasonable means to determine that
55 a request to exercise any of the rights afforded under subdivisions (1) to
56 (4), inclusive, of subsection (a) of section 42-518, as amended by this act,
57 is being made by, or on behalf of, the consumer who is entitled to
58 exercise such consumer rights with respect to the personal data at issue.

59 (4) "Biometric data" means data generated by automatic
60 measurements of an individual's biological characteristics, such as a
61 fingerprint, a voiceprint, eye retinas, irises or other unique biological
62 patterns or characteristics that are used to identify a specific individual.
63 "Biometric data" does not include (A) a digital or physical photograph,
64 (B) an audio or video recording, or (C) any data generated from a digital
65 or physical photograph, or an audio or video recording, unless such
66 data [is] are generated to identify a specific individual.

67 (5) "Business associate" has the same meaning as provided in HIPAA.

68 (6) "Child" has the same meaning as provided in COPPA.

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

79 (8) "Consumer" means an individual who is a resident of this state.
80 "Consumer" does not include an individual acting in a commercial or
81 employment context or as an employee, owner, director, officer or
82 contractor of a company, partnership, sole proprietorship, nonprofit
83 organization or government agency whose communications or
84 transactions with the controller occur solely within the context of that
85 individual's role with the company, partnership, sole proprietorship,
86 nonprofit organization or government agency.

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

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

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

96 (12) "COPPA" means the Children's Online Privacy Protection Act of
97 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and
98 exemptions adopted pursuant to said act, as said act and such
99 regulations, rules, guidance and exemptions may be amended from

100 time to time.

101 (13) "Covered entity" has the same meaning as provided in HIPAA.

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

106 (15) ["Decisions that produce legal or similarly significant effects
107 concerning the consumer"] "Decision that produces any legal or
108 similarly significant effect" means [decisions] any decision made by the
109 controller, or on behalf of the controller, that [result] results in the
110 provision or denial by the controller of any financial or lending
111 [services,] service, any housing, any insurance, any education
112 enrollment or opportunity, any criminal justice, any employment
113 [opportunities,] opportunity, any health care [services] service or access
114 to any essential [goods or services] good or service.

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

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

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

129 (19) "Geofence" means any technology that uses global positioning

130 coordinates, cell tower connectivity, cellular data, radio frequency
131 identification, wireless fidelity technology data or any other form of
132 location detection, or any combination of such coordinates, connectivity,
133 data, identification or other form of location detection, to establish a
134 virtual boundary.

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

138 (21) "Identified or identifiable individual" means an individual who
139 can be readily identified, directly or indirectly.

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

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

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

149 [(24)] (25) "Nonprofit organization" means any organization that is
150 exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or
151 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent
152 corresponding internal revenue code of the United States, as amended
153 from time to time.

154 [(25)] (26) "Person" means an individual, association, company,
155 limited liability company, corporation, partnership, sole proprietorship,
156 trust or other legal entity.

157 [(26)] (27) "Personal data" means any information that is linked or
158 reasonably linkable to an identified or identifiable individual. "Personal

159 data" does not include de-identified data or publicly available
160 information.

161 [(27)] (28) "Precise geolocation data" means information derived from
162 technology, including, but not limited to, global positioning system
163 level latitude and longitude coordinates or other mechanisms, that
164 directly identifies the specific location of an individual with precision
165 and accuracy within a radius of one thousand seven hundred fifty feet.
166 "Precise geolocation data" does not include the content of
167 communications or any data generated by or connected to advanced
168 utility metering infrastructure systems or equipment for use by a utility.

169 [(28)] (29) "Process" and "processing" mean any operation or set of
170 operations performed, whether by manual or automated means, on
171 personal data or on sets of personal data, such as the collection, use,
172 storage, disclosure, analysis, deletion or modification of personal data.

173 [(29)] (30) "Processor" means a person who processes personal data
174 on behalf of a controller.

175 [(30)] (31) "Profiling" means any form of automated processing
176 performed on personal data to evaluate, analyze or predict personal
177 aspects related to an identified or identifiable individual's economic
178 situation, health, personal preferences, interests, reliability, behavior,
179 location or movements.

180 [(31)] (32) "Protected health information" has the same meaning as
181 provided in HIPAA.

182 [(32)] (33) "Pseudonymous data" means personal data that cannot be
183 attributed to a specific individual without the use of additional
184 information, provided such additional information is kept separately
185 and is subject to appropriate technical and organizational measures to
186 ensure that the personal data [is] are not attributed to an identified or
187 identifiable individual.

188 [(33)] (34) "Publicly available information" (A) means information

189 that [(A)] (i) is lawfully made available [through] from federal, state or
190 municipal government records, or [widely distributed media, and (B)]
191 (ii) a controller has a reasonable basis to believe (I) a consumer has
192 lawfully made available to the general public, or (II) has been lawfully
193 made available to the general public from widely distributed media, and
194 (B) does not include (i) any biometric data that can be associated with a
195 specific consumer and were collected without the consumer's consent,
196 or (ii) any information concerning a consumer that is lawfully made
197 available by a person to whom the consumer disclosed the information.

198 [(34)] (35) "Reproductive or sexual health care" means any health
199 care-related services or products rendered or provided concerning a
200 consumer's reproductive system or sexual well-being, including, but not
201 limited to, any such service or product rendered or provided concerning
202 (A) an individual health condition, status, disease, diagnosis, diagnostic
203 test or treatment, (B) a social, psychological, behavioral or medical
204 intervention, (C) a surgery or procedure, including, but not limited to,
205 an abortion, (D) a use or purchase of a medication, including, but not
206 limited to, a medication used or purchased for the purposes of an
207 abortion, (E) a bodily function, vital sign or symptom, (F) a
208 measurement of a bodily function, vital sign or symptom, or (G) an
209 abortion, including, but not limited to, medical or nonmedical services,
210 products, diagnostics, counseling or follow-up services for an abortion.

211 [(35)] (36) "Reproductive or sexual health data" means any personal
212 data concerning an effort made by a consumer to seek, or a consumer's
213 receipt of, reproductive or sexual health care.

214 [(36)] (37) "Reproductive or sexual health facility" means any health
215 care facility in which at least seventy per cent of the health care-related
216 services or products rendered or provided in such facility are
217 reproductive or sexual health care.

218 [(37)] (38) "Sale of personal data" means the exchange of personal data
219 for monetary or other valuable consideration by the controller to a third
220 party. "Sale of personal data" does not include (A) the disclosure of

221 personal data to a processor that processes the personal data on behalf
222 of the controller, (B) the disclosure of personal data to a third party for
223 purposes of providing a product or service requested by the consumer,
224 (C) the disclosure or transfer of personal data to an affiliate of the
225 controller, (D) the disclosure of personal data where the consumer
226 directs the controller to disclose the personal data or intentionally uses
227 the controller to interact with a third party, (E) the disclosure of personal
228 data that the consumer (i) intentionally made available to the general
229 public via a channel of mass media, and (ii) did not restrict to a specific
230 audience, or (F) the disclosure or transfer of personal data to a third
231 party as an asset that is part of a merger, acquisition, bankruptcy or
232 other transaction, or a proposed merger, acquisition, bankruptcy or
233 other transaction, in which the third party assumes control of all or part
234 of the controller's assets.

235 [(38)] (39) "Sensitive data" means personal data that includes (A) data
236 revealing (i) racial or ethnic origin, (ii) religious beliefs, (iii) a mental or
237 physical health condition, [or] diagnosis, disability or treatment, (iv) sex
238 life, sexual orientation or status as nonbinary or transgender, or (v)
239 citizenship or immigration status, (B) consumer health data, (C) [the
240 processing of] genetic or biometric data [for the purpose of uniquely
241 identifying an individual] or information derived therefrom, (D)
242 personal data collected from [a known] an individual the controller has
243 actual knowledge, or knowledge fairly implied on the basis of objective
244 circumstances, is a child, (E) data concerning an individual's status as a
245 victim of crime, as defined in section 1-1k, [or] (F) precise geolocation
246 data, (G) neural data, (H) a consumer's financial account number,
247 financial account log-in information or credit card or debit card number
248 that, in combination with any required access or security code,
249 password or credential, would allow access to a consumer's financial
250 account, or (I) government-issued identification number, including, but
251 not limited to, Social Security number, passport number, state
252 identification card number or driver's license number, that applicable
253 law does not require to be publicly displayed.

254 [(39)] (40) "Targeted advertising" means displaying advertisements to
255 a consumer where the advertisement is selected based on personal data
256 obtained or inferred from that consumer's activities over time and across
257 nonaffiliated Internet web sites or online applications to predict such
258 consumer's preferences or interests. "Targeted advertising" does not
259 include (A) advertisements based on activities within a controller's own
260 Internet web sites or online applications, (B) advertisements based on
261 the context of a consumer's current search query, visit to an Internet web
262 site or online application, (C) advertisements directed to a consumer in
263 response to the consumer's request for information or feedback, or (D)
264 processing personal data solely to measure or report advertising
265 frequency, performance or reach.

266 [(40)] (41) "Third party" means a person, such as a public authority,
267 agency or body, other than the consumer, controller or processor or an
268 affiliate of the processor or the controller.

269 [(41)] (42) "Trade secret" has the same meaning as provided in section
270 35-51.

271 Sec. 3. Section 42-516 of the general statutes is repealed and the
272 following is substituted in lieu thereof (*Effective October 1, 2025*):

273 The provisions of sections 42-515 to 42-525, inclusive, as amended by
274 this act, apply to persons that: [conduct] (1) Conduct business in this
275 state, or [persons that] produce products or services that are targeted to
276 residents of this state, and [that] during the preceding calendar year [:
277 (1) Controlled] controlled or processed the personal data of not [less]
278 fewer than [one hundred thousand] thirty-five thousand consumers,
279 excluding personal data controlled or processed solely for the purpose
280 of completing a payment transaction; [or (2) controlled or processed the
281 personal data of not less than twenty-five thousand consumers and
282 derived more than twenty-five per cent of their gross revenue from the
283 sale of personal data] (2) control or process consumers' sensitive data;
284 or (3) offer consumers' personal data for sale in trade or commerce.

285 Sec. 4. Subsections (a) and (b) of section 42-517 of the general statutes
286 are repealed and the following is substituted in lieu thereof (*Effective*
287 *October 1, 2025*):

288 (a) The provisions of sections 42-515 to 42-525, inclusive, as amended
289 by this act, do not apply to any: (1) Body, authority, board, bureau,
290 commission, district or agency of this state or of any political
291 subdivision of this state; (2) person who has entered into a contract with
292 any body, authority, board, bureau, commission, district or agency
293 described in subdivision (1) of this subsection while such person is
294 processing consumer health data on behalf of such body, authority,
295 board, bureau, commission, district or agency pursuant to such contract;
296 (3) [nonprofit organization] candidate committee, national committee,
297 party committee or political committee, as such terms are defined in
298 section 9-601; (4) institution of higher education; (5) national securities
299 association that is registered under 15 USC 78o-3 of the Securities
300 Exchange Act of 1934, as amended from time to time; (6) [financial
301 institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15
302 USC 6801 et seq.; (7) covered entity or business associate, as defined in
303 45 CFR 160.103; (8)] tribal nation government organization; [or (9)] (7)
304 air carrier, as defined in 49 USC 40102, as amended from time to time,
305 and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et
306 seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts
307 may be amended from time to time; (8) insurer, as defined in section
308 38a-1, fraternal benefit society, within the meaning of section 38a-595,
309 health carrier, as defined in section 38a-591a, insurance-support
310 organization, as defined in section 38a-976, or insurance agent or
311 insurance producer, as such terms are defined in section 38a-702a, that
312 is regulated by the Insurance Department and in compliance with all
313 applicable requirements established by the Insurance Commissioner
314 concerning personal data; (9) bank, Connecticut credit union, federal
315 credit union, out-of-state bank or out-of-state credit union, or any
316 affiliate or subsidiary thereof, as such terms are defined in section 36a-
317 2, that is regulated by the Department of Banking and in compliance
318 with all applicable requirements established by the Banking

319 Commissioner concerning personal data; or (10) agent, broker-dealer,
320 investment adviser or investment adviser agent, as such terms are
321 defined in section 36b-3, who is regulated by the Department of Banking
322 or the Securities and Exchange Commission and is in compliance with
323 all applicable requirements established by the Banking Commissioner
324 or the Securities and Exchange Commission concerning personal data.

325 (b) The following information and data [is] are exempt from the
326 provisions of sections 42-515 to 42-526, inclusive, as amended by this
327 act: (1) Protected health information under HIPAA; (2) patient-
328 identifying information for purposes of 42 USC 290dd-2; (3) identifiable
329 private information for purposes of the federal policy for the protection
330 of human subjects under 45 CFR 46; (4) identifiable private information
331 that is otherwise information collected as part of human subjects
332 research pursuant to the good clinical practice guidelines issued by the
333 International Council for Harmonization of Technical Requirements for
334 Pharmaceuticals for Human Use; (5) personal data for purposes of the
335 protection of human subjects under 21 CFR Parts 6, 50 and 56, or
336 personal data used or shared in research, as defined in 45 CFR 164.501,
337 that is conducted in accordance with the standards set forth in this
338 subdivision and subdivisions (3) and (4) of this subsection, or other
339 research conducted in accordance with applicable law; (6) information
340 and documents created for purposes of the Health Care Quality
341 Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work
342 product for purposes of section 19a-127o and the Patient Safety and
343 Quality Improvement Act, 42 USC 299b-21 et seq., as amended from
344 time to time; (8) information derived from any of the health care-related
345 information listed in this subsection that is de-identified in accordance
346 with the requirements for de-identification pursuant to HIPAA; (9)
347 information originating from and intermingled to be indistinguishable
348 with, or information treated in the same manner as, information exempt
349 under this subsection that is maintained by a covered entity or business
350 associate, program or qualified service organization, as specified in 42
351 USC 290dd-2, as amended from time to time; (10) information used for
352 public health activities and purposes as authorized by HIPAA,

353 community health activities and population health activities; (11) the
354 collection, maintenance, disclosure, sale, communication or use of any
355 personal information bearing on a consumer's credit worthiness, credit
356 standing, credit capacity, character, general reputation, personal
357 characteristics or mode of living by a consumer reporting agency,
358 furnisher or user that provides information for use in a consumer report,
359 and by a user of a consumer report, but only to the extent that such
360 activity is regulated by and authorized under the Fair Credit Reporting
361 Act, 15 USC 1681 et seq., as amended from time to time; (12) personal
362 data collected, processed, sold or disclosed in compliance with the
363 Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended
364 from time to time; (13) personal data regulated by the Family
365 Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended
366 from time to time; (14) personal data collected, processed, sold or
367 disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq.,
368 as amended from time to time; (15) data processed or maintained (A) in
369 the course of an individual applying to, employed by or acting as an
370 agent or independent contractor of a controller, processor, consumer
371 health data controller or third party, to the extent that the data [is] are
372 collected and used within the context of that role, (B) as the emergency
373 contact information of an individual under sections 42-515 to 42-526,
374 inclusive, as amended by this act, used for emergency contact purposes,
375 or (C) that [is] are necessary to retain to administer benefits for another
376 individual relating to the individual who is the subject of the
377 information under subdivision (1) of this subsection and used for the
378 purposes of administering such benefits; [and] (16) personal data
379 collected, processed, sold or disclosed in relation to price, route or
380 service, as such terms are used in the Federal Aviation Act of 1958, 49
381 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC
382 41713, as said acts may be amended from time to time; (17) data subject
383 to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as
384 amended from time to time; and (18) information included in a limited
385 data set, as described in 45 CFR 164.514(e), as amended from time to
386 time, to the extent such information is used, disclosed and maintained
387 in the manner specified in 45 CFR 164.514(e), as amended from time to

388 time.

389 Sec. 5. Section 42-518 of the general statutes is repealed and the
390 following is substituted in lieu thereof (*Effective October 1, 2025*):

391 (a) A consumer shall have the right to: (1) Confirm whether or not a
392 controller is processing the consumer's personal data and access such
393 personal data, including, but not limited to, any inferences about the
394 consumer derived from such personal data and whether a controller or
395 processor is processing a consumer's personal data for the purposes of
396 profiling to make a decision that produces any legal or similarly
397 significant effect concerning a consumer, unless such confirmation or
398 access would require the controller to reveal a trade secret or the
399 controller is prohibited from disclosing such personal data under
400 subsection (e) of this section; (2) correct inaccuracies in the consumer's
401 personal data, taking into account the nature of the personal data and
402 the purposes of the processing of the consumer's personal data; (3)
403 delete personal data provided by, or obtained about, the consumer; (4)
404 obtain a copy of the consumer's personal data processed by the
405 controller, in a portable and, to the extent technically feasible, readily
406 usable format that allows the consumer to transmit the data to another
407 controller without hindrance, where the processing is carried out by
408 automated means, provided such controller shall not be required to
409 reveal any trade secret; [and] (5) opt out of the processing of the personal
410 data for purposes of (A) targeted advertising, (B) the sale of personal
411 data, except as provided in subdivision (2) of subsection [(b)] (a) of
412 section 42-520, as amended by this act, or (C) profiling in furtherance of
413 [solely] any automated [decisions that produce] decision that produces
414 any legal or similarly significant [effects] effect concerning the
415 consumer; (6) if the consumer's personal data were processed for the
416 purposes of profiling in furtherance of any automated decision that
417 produced any legal or similarly significant effect concerning the
418 consumer, and if feasible, (A) question the result of such profiling, (B)
419 be informed of the reason that such profiling resulted in such decision,
420 (C) review the consumer's personal data that were processed for the

421 purposes of such profiling, and (D) if the profiling decision concerned
422 housing, taking into account the nature of the personal data and the
423 purposes for which such personal data were processed, allow the
424 consumer to correct any incorrect personal data that were processed for
425 the purposes of such profiling and have the profiling decision
426 reevaluated based on the corrected personal data; and (7) obtain from
427 the controller a list of the third parties to which such controller has sold
428 the consumer's personal data or, if such controller does not maintain a
429 list of the third parties to which such controller has sold the consumer's
430 personal data, a list of all third parties to which such controller has sold
431 personal data, provided the controller shall not be required to reveal any
432 trade secret.

433 (b) A consumer may exercise rights under this section by a secure and
434 reliable means established by the controller and described to the
435 consumer in the controller's privacy notice. A consumer may designate
436 an authorized agent in accordance with section 42-519 to exercise the
437 rights of such consumer to opt out of the processing of such consumer's
438 personal data for purposes of subdivision (5) of subsection (a) of this
439 section on behalf of the consumer. In the case of processing personal
440 data of a [known] consumer who the controller has actual knowledge,
441 or knowledge fairly implied on the basis of objective circumstances, is a
442 child, the parent or legal guardian may exercise such consumer rights
443 on the child's behalf. In the case of processing personal data concerning
444 a consumer subject to a guardianship, conservatorship or other
445 protective arrangement, the guardian or the conservator of the
446 consumer may exercise such rights on the consumer's behalf.

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

451 (1) A controller shall respond to the consumer without undue delay,
452 but not later than forty-five days after receipt of the request. The
453 controller may extend the response period by forty-five additional days

454 when reasonably necessary, considering the complexity and number of
455 the consumer's requests, provided the controller informs the consumer
456 of any such extension within the initial forty-five-day response period
457 and of the reason for the extension.

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

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

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

487 that such controller shall not comply with such request.

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

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

511 (e) A controller shall not disclose the following personal data in
512 response to a request to exercise the consumer's rights under
513 subdivision (1) of subsection (a) of this section, and shall instead inform
514 the consumer or the person exercising such right on behalf of the
515 consumer, with sufficient particularity, that the controller has collected
516 such personal data: (1) The consumer's Social Security number; (2) the
517 consumer's driver's license number, state identification card number or
518 other government-issued identification number; (3) the consumer's
519 financial account number; (4) the consumer's health insurance

520 identification number or medical identification number; (5) the
521 consumer's account password; (6) the consumer's security question or
522 answer thereto; or (7) the consumer's biometric data.

523 Sec. 6. Section 42-520 of the general statutes is repealed and the
524 following is substituted in lieu thereof (*Effective October 1, 2025*):

525 (a) (1) A controller shall: [(1)] (A) Limit the collection of personal data
526 to what is [adequate, relevant and] reasonably necessary and
527 proportionate in relation to the purposes for which such data [is] are
528 processed, as disclosed to the consumer; [(2) except as otherwise
529 provided in sections 42-515 to 42-525, inclusive] (B) unless the controller
530 obtains the consumer's consent, not process the consumer's personal
531 data for [purposes] any material new purpose that [are] is neither
532 reasonably necessary to, nor compatible with, the [disclosed] purposes
533 [for which such personal data is processed, as] that were disclosed to the
534 consumer [unless the controller obtains the consumer's consent; (3)]
535 pursuant to subparagraph (A) of this subdivision, taking into account
536 (i) the consumer's reasonable expectation regarding such personal data
537 at the time such personal data were collected based on the purposes that
538 were disclosed to the consumer pursuant to subparagraph (A) of this
539 subdivision, (ii) the relationship that such material new purpose bears
540 to the purposes that were disclosed to the consumer pursuant to
541 subparagraph (A) of this subdivision, (iii) the impact that processing
542 such personal data for such material new purpose might have on the
543 consumer, (iv) the relationship between the consumer and the controller
544 and the context in which the personal data were collected, and (v) the
545 existence of additional safeguards, including, but not limited to,
546 encryption or pseudonymization, in processing such personal data for
547 such material new purpose; (C) establish, implement and maintain
548 reasonable administrative, technical and physical data security practices
549 to protect the confidentiality, integrity and accessibility of personal data
550 appropriate to the volume and nature of the personal data at issue; [(4)]
551 (D) not process sensitive data concerning a consumer unless such
552 processing is reasonably necessary and proportionate in relation to the

553 purposes for which such sensitive data are processed and without
554 obtaining the consumer's consent, or, in the case of the processing of
555 sensitive data concerning a [known] consumer who the controller has
556 actual knowledge, or knowledge fairly implied on the basis of objective
557 circumstances, is a child, without processing such data in accordance
558 with COPPA; [(5)] (E) not process personal data in violation of [the laws]
559 any law of this state [and federal laws that prohibit] that prohibits
560 unlawful discrimination against consumers, and any evidence, or lack
561 of evidence, concerning proactive anti-bias testing or any similar
562 proactive effort to avoid processing such data in violation of such law,
563 including, but not limited to, any evidence or lack of evidence
564 concerning the quality, efficacy, recency and scope of any such testing
565 or effort, the results of such testing or effort and the response to the
566 results of such testing or effort, shall be relevant to any claim available
567 for a violation of such law and any defense available thereto; (F) not
568 process personal data in violation of any federal law that prohibits
569 unlawful discrimination against consumers; [(6)] (G) provide an
570 effective mechanism for a consumer to revoke the consumer's consent
571 under this section that is at least as easy as the mechanism by which the
572 consumer provided the consumer's consent and, upon revocation of
573 such consent, cease to process the data as soon as practicable, but not
574 later than fifteen days after the receipt of such request; (H) not sell the
575 sensitive data of a consumer without the consumer's consent; and [(7)]
576 (I) not process the personal data of a consumer for purposes of targeted
577 advertising, or sell the consumer's personal data, [without the
578 consumer's consent,] under circumstances where a controller has actual
579 knowledge, or [wilfully disregards] knowledge fairly implied on the
580 basis of objective circumstances, that the consumer is at least thirteen
581 years of age but younger than [sixteen] eighteen years of age. A
582 controller shall not discriminate against a consumer for exercising any
583 of the consumer rights contained in sections 42-515 to 42-525, inclusive,
584 as amended by this act, including denying goods or services, charging
585 different prices or rates for goods or services or providing a different
586 level of quality of goods or services to the consumer.

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

596 [(c)] (b) (1) A controller shall provide consumers with a reasonably
597 accessible, clear and meaningful privacy notice that includes: [(1)] (A)
598 The categories of personal data processed by the controller; [(2)] (B) the
599 purpose for processing personal data; [(3) how consumers may exercise
600 their consumer rights, including how a consumer may appeal a
601 controller's decision] (C) a description of the means, established
602 pursuant to subsection (c) of this section, for consumers to submit
603 requests to exercise their consumer rights pursuant to sections 42-515 to
604 42-525, inclusive, as amended by this act, including, but not limited to,
605 a description of (i) how consumers may exercise their consumer rights
606 under subsection (a) of section 42-518, as amended by this act, and (ii)
607 how consumers may appeal controllers' decisions with regard to [the
608 consumer's request; (4)] requests to exercise such rights; (D) the
609 categories of personal data that the controller [shares with] sells to third
610 parties, if any; [(5)] (E) the categories of third parties, if any, [with] to
611 which the controller [shares] sells personal data; [and (6)] (F) a clear and
612 conspicuous disclosure of (i) any processing of personal data for
613 purposes of targeted advertising, or (ii) any sale of personal data to a
614 third party for purposes of targeted advertising; (G) an active electronic
615 mail address or other online mechanism that [the consumer] consumers
616 may use to contact the controller; (H) a statement disclosing whether the
617 controller collects, uses or sells personal data for the purpose of training
618 large language models; and (I) the most recent month and year during
619 which the controller updated such privacy notice.

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

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

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

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

657 [(e)] (c) (1) A controller shall establish [, and shall describe in a
658 privacy notice,] one or more secure and reliable means for consumers to
659 submit a request to exercise their consumer rights pursuant to sections
660 42-515 to 42-525, inclusive, as amended by this act. Such means shall
661 take into account the ways in which consumers normally interact with
662 the controller, the need for secure and reliable communication of such
663 requests and the ability of the controller to verify the identity of the
664 consumer making the request. A controller shall not require a consumer
665 to create a new account in order to exercise consumer rights, but may
666 require a consumer to use an existing account. Any such means shall
667 include:

668 (A) (i) Providing a clear and conspicuous [link] hyperlink on the
669 controller's Internet web site that is clearly labeled "your opt-out rights",
670 "your privacy rights" or with similar language and (I) directly allows a
671 request made by a consumer, or an agent of the consumer, to opt out of
672 the processing of the consumer's personal data for purposes targeted
673 advertising, or any sale of the consumer's personal data, or (II) redirects
674 the consumer, or an agent of the consumer, to an Internet web page that
675 enables [a] the consumer [,] or [an] such agent [of the consumer,] to opt
676 out of the processing of the consumer's personal data for purposes of
677 targeted advertising, or any sale of the consumer's personal data; and

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

- 685 (I) Not unfairly disadvantage another controller;
- 686 (II) Not make use of a default setting, but, rather, require the
687 consumer to make an affirmative, freely given and unambiguous choice
688 to opt out of any processing of such consumer's personal data pursuant
689 to sections 42-515 to 42-525, inclusive, as amended by this act;
- 690 (III) Be consumer-friendly and easy to use by the average consumer;
- 691 (IV) Be as consistent as possible with any other similar platform,
692 technology or mechanism required by any federal or state law or
693 regulation; and
- 694 (V) Enable the controller to accurately determine whether the
695 consumer is a resident of this state and whether the consumer has made
696 a legitimate request to opt out of any sale of such consumer's personal
697 data or targeted advertising.
- 698 (B) If a consumer's decision to opt out of any processing of the
699 consumer's personal data for the purposes of targeted advertising, or
700 any sale of such personal data, through an opt-out preference signal sent
701 in accordance with the provisions of subparagraph (A) of this
702 subdivision conflicts with the consumer's existing controller-specific
703 privacy setting or voluntary participation in a controller's bona fide
704 loyalty, rewards, premium features, discounts or club card program, the
705 controller shall comply with such consumer's opt-out preference signal
706 but may notify such consumer of such conflict and provide to such
707 consumer the choice to confirm such controller-specific privacy setting
708 or participation in such program.
- 709 (2) If a controller responds to consumer opt-out requests received
710 pursuant to subparagraph (A) of subdivision (1) of this subsection by
711 informing the consumer of a charge for the use of any product or service,
712 the controller shall present the terms of any financial incentive offered
713 pursuant to subdivision (2) of subsection [(b)] (a) of this section for the
714 retention, use, sale or sharing of the consumer's personal data.

715 Sec. 7. Section 42-521 of the general statutes is repealed and the
716 following is substituted in lieu thereof (*Effective October 1, 2025*):

717 (a) A processor shall adhere to the instructions of a controller and
718 shall assist the controller in meeting the controller's obligations under
719 sections 42-515 to 42-525, inclusive, as amended by this act. Such
720 assistance shall include: (1) Taking into account the nature of processing
721 and [the information available to the processor, by appropriate technical
722 and organizational measures,] insofar as is [reasonably practicable]
723 possible, to fulfill the controller's obligation to respond to [consumer
724 rights requests] consumers' requests to exercise their rights under
725 section 42-518, as amended by this act; (2) taking into account the nature
726 of processing and the information available to the processor, by
727 assisting the controller in meeting the controller's obligations in relation
728 to the security of processing the personal data and in relation to the
729 notification of a breach of security, as defined in section 36a-701b, of the
730 system of the processor, in order to meet the controller's obligations; and
731 (3) providing necessary information to enable the controller to conduct
732 and document data protection assessments and impact assessments.

733 (b) A contract between a controller and a processor shall govern the
734 processor's data processing procedures with respect to processing
735 performed on behalf of the controller. The contract shall be binding and
736 clearly set forth instructions for processing data, the nature and purpose
737 of processing, the type of data subject to processing, the duration of
738 processing and the rights and obligations of both parties. The contract
739 shall also require that the processor: (1) Ensure that each person
740 processing personal data is subject to a duty of confidentiality with
741 respect to the data; (2) at the controller's direction, delete or return all
742 personal data to the controller as requested at the end of the provision
743 of services, unless retention of the personal data is required by law; (3)
744 upon the reasonable request of the controller, make available to the
745 controller all information in its possession necessary to demonstrate the
746 processor's compliance with the obligations in sections 42-515 to 42-525,
747 inclusive, as amended by this act; (4) after providing the controller an

748 opportunity to object, engage any subcontractor pursuant to a written
749 contract that requires the subcontractor to meet the obligations of the
750 processor with respect to the personal data; and (5) allow, and cooperate
751 with, reasonable assessments by the controller or the controller's
752 designated assessor, or the processor may arrange for a qualified and
753 independent assessor to conduct an assessment of the processor's
754 policies and technical and organizational measures in support of the
755 obligations under sections 42-515 to 42-525, inclusive, as amended by
756 this act, using an appropriate and accepted control standard or
757 framework and assessment procedure for such assessments. The
758 processor shall provide a report of such assessment to the controller
759 upon request.

760 (c) Nothing in this section shall be construed to relieve a controller or
761 processor from the liabilities imposed on the controller or processor by
762 virtue of such controller's or processor's role in the processing
763 relationship, as described in sections 42-515 to 42-525, inclusive, as
764 amended by this act.

765 (d) Determining whether a person is acting as a controller or
766 processor with respect to a specific processing of data is a fact-based
767 determination that depends upon the context in which personal data [is]
768 are to be processed. A person who is not limited in such person's
769 processing of personal data pursuant to a controller's instructions, or
770 who fails to adhere to such instructions, is a controller and not a
771 processor with respect to a specific processing of data. A processor that
772 continues to adhere to a controller's instructions with respect to a
773 specific processing of personal data remains a processor. If a processor
774 begins, alone or jointly with others, determining the purposes and
775 means of the processing of personal data, the processor is a controller
776 with respect to such processing and may be subject to an enforcement
777 action under section 42-525.

778 Sec. 8. Section 42-522 of the general statutes is repealed and the
779 following is substituted in lieu thereof (*Effective October 1, 2025*):

780 (a) For the purposes of this section, processing that presents a
781 heightened risk of harm to a consumer includes: (1) The processing of
782 personal data for the purposes of targeted advertising; (2) the sale of
783 personal data; (3) the processing of personal data for the purposes of
784 profiling, where such profiling presents a reasonably foreseeable risk of
785 (A) unfair or deceptive treatment of, or unlawful disparate impact on,
786 consumers, (B) financial, physical or reputational injury to consumers,
787 (C) a physical or other intrusion upon the solitude or seclusion, or the
788 private affairs or concerns, of consumers, where such intrusion would
789 be offensive to a reasonable person, or (D) other substantial injury to
790 consumers; and (4) the processing of sensitive data.

791 [(a)] (b) (1) A controller shall conduct and document a data protection
792 assessment for each of the controller's processing activities that presents
793 a heightened risk of harm to a consumer. [For the purposes of this
794 section, processing that presents a heightened risk of harm to a
795 consumer includes: (1) The processing of personal data for the purposes
796 of targeted advertising; (2) the sale of personal data; (3) the processing
797 of personal data for the purposes of profiling, where such profiling
798 presents a reasonably foreseeable risk of (A) unfair or deceptive
799 treatment of, or unlawful disparate impact on, consumers, (B) financial,
800 physical or reputational injury to consumers, (C) a physical or other
801 intrusion upon the solitude or seclusion, or the private affairs or
802 concerns, of consumers, where such intrusion would be offensive to a
803 reasonable person, or (D) other substantial injury to consumers; and (4)
804 the processing of sensitive data.]

805 [(b) Data protection assessments] (2) Each data protection assessment
806 conducted pursuant to subdivision (1) of this subsection [(a) of this
807 section] shall identify and weigh the benefits that may flow, directly and
808 indirectly, from the processing to the controller, the consumer, other
809 stakeholders and the public against the potential risks to the rights of
810 the consumer associated with such processing, as mitigated by
811 safeguards that can be employed by the controller to reduce such risks.
812 The controller shall factor into [any] each such data protection

813 assessment the use of de-identified data and the reasonable expectations
814 of consumers, as well as the context of the processing and the
815 relationship between the controller and the consumer whose personal
816 data will be processed.

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

842 [(c)] (d) The Attorney General may require that a controller disclose
843 any data protection assessment or impact assessment that is relevant to
844 an investigation conducted by the Attorney General, and the controller
845 shall make the data protection assessment or impact assessment

846 available to the Attorney General. The Attorney General may evaluate
847 the data protection assessment or impact assessment for compliance
848 with the responsibilities set forth in sections 42-515 to 42-525, inclusive,
849 as amended by this act. Data protection assessments and impact
850 assessments shall be confidential and shall be exempt from disclosure
851 under the Freedom of Information Act, as defined in section 1-200. To
852 the extent any information contained in a data protection assessment or
853 impact assessment disclosed to the Attorney General includes
854 information subject to attorney-client privilege or work product
855 protection, such disclosure shall not constitute a waiver of such
856 privilege or protection.

857 [(d)] (e) A single data protection assessment or impact assessment
858 may address a comparable set of processing operations that include
859 similar activities.

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

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

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

873 Sec. 9. Subsections (a) to (d), inclusive, of section 42-524 of the general
874 statutes are repealed and the following are substituted in lieu thereof
875 (*Effective October 1, 2025*):

876 (a) Nothing in sections 42-515 to 42-526, inclusive, as amended by this

877 act, shall be construed to restrict a controller's, processor's or consumer
878 health data controller's ability to: (1) Comply with federal, state or
879 municipal ordinances or regulations; (2) comply with a civil, criminal or
880 regulatory inquiry, investigation, subpoena or summons by federal,
881 state, municipal or other governmental authorities; (3) cooperate with
882 law enforcement agencies concerning conduct or activity that the
883 controller, processor or consumer health data controller reasonably and
884 in good faith believes may violate federal, state or municipal ordinances
885 or regulations; (4) investigate, establish, exercise, prepare for or defend
886 legal claims; (5) provide a product or service specifically requested by a
887 consumer; (6) perform under a contract to which a consumer is a party,
888 including fulfilling the terms of a written warranty; (7) take steps at the
889 request of a consumer prior to entering into a contract; (8) take
890 immediate steps to protect an interest that is essential for the life or
891 physical safety of the consumer or another individual, and where the
892 processing cannot be manifestly based on another legal basis; (9)
893 prevent, detect, protect against or respond to security incidents, identity
894 theft, fraud, harassment, malicious or deceptive activities or any illegal
895 activity, preserve the integrity or security of systems or investigate,
896 report or prosecute those responsible for any such action; (10) engage in
897 public or peer-reviewed scientific or statistical research in the public
898 interest that adheres to all other applicable ethics and privacy laws and
899 is approved, monitored and governed by an institutional review board
900 that determines, or similar independent oversight entities that
901 determine, (A) whether the deletion of the information is likely to
902 provide substantial benefits that do not exclusively accrue to the
903 controller or consumer health data controller, (B) the expected benefits
904 of the research outweigh the privacy risks, and (C) whether the
905 controller or consumer health data controller has implemented
906 reasonable safeguards to mitigate privacy risks associated with
907 research, including any risks associated with re-identification; (11) assist
908 another controller, processor, consumer health data controller or third
909 party with any of the obligations under sections 42-515 to 42-526,
910 inclusive, as amended by this act; or (12) process personal data for
911 reasons of public interest in the area of public health, community health

912 or population health, but solely to the extent that such processing is (A)
913 subject to suitable and specific measures to safeguard the rights of the
914 consumer whose personal data [is] are being processed, and (B) under
915 the responsibility of a professional subject to confidentiality obligations
916 under federal, state or local law.

917 (b) The obligations imposed on controllers, processors or consumer
918 health data controllers under sections 42-515 to 42-526, inclusive, as
919 amended by this act, shall not restrict a controller's, processor's or
920 consumer health data controller's ability to collect, use or retain data for
921 internal use to: (1) Conduct internal research to develop, improve or
922 repair products, services or technology; (2) effectuate a product recall;
923 (3) identify and repair technical errors that impair existing or intended
924 functionality; (4) process personal data for the purposes of profiling in
925 furtherance of any automated decision that may produce any legal or
926 similarly significant effect concerning a consumer, provided such
927 personal data are (A) processed only to the extent necessary to detect or
928 correct any bias that may result from processing such data for such
929 purposes, such bias cannot effectively be detected or corrected without
930 processing such data and such data are deleted once such processing
931 has been completed, (B) processed subject to appropriate safeguards to
932 protect the rights of consumers secured by the Constitution or laws of
933 this state or of the United States, (C) subject to technical restrictions
934 concerning the reuse of such data and state-of-the-art security and
935 privacy measures, including, but not limited to, pseudonymization, (D)
936 subject to measures to ensure that such data are secure, protected and
937 subject to suitable safeguards, including, but not limited to, strict
938 controls concerning, and documentation of, access to such data, to avoid
939 misuse and ensure that only authorized persons may access such data
940 while preserving the confidentiality of such data, and (E) not
941 transmitted, transferred or otherwise accessed by any third party; or
942 [(4)] (5) perform solely internal operations that are reasonably aligned
943 with the expectations of the consumer or reasonably anticipated based
944 on the consumer's existing relationship with the controller or consumer
945 health data controller, or are otherwise compatible with processing data

946 in furtherance of the provision of a product or service specifically
947 requested by a consumer or the performance of a contract to which the
948 consumer is a party.

949 (c) The obligations imposed on controllers, processors or consumer
950 health data controllers under sections 42-515 to 42-526, inclusive, as
951 amended by this act, shall not apply where compliance by the controller,
952 processor or consumer health data controller with said sections would
953 violate an evidentiary privilege under the laws of this state. Nothing in
954 sections 42-515 to 42-526, inclusive, as amended by this act, shall be
955 construed to prevent a controller, processor or consumer health data
956 controller from providing personal data concerning a consumer to a
957 person covered by an evidentiary privilege under the laws of the state
958 as part of a privileged communication.

959 (d) A controller, processor or consumer health data controller that
960 discloses personal data to a processor or third-party controller in
961 accordance with sections 42-515 to 42-526, inclusive, as amended by this
962 act, shall not be deemed to have violated said sections if the processor
963 or third-party controller that receives and processes such personal data
964 violates said sections, provided, at the time the disclosing controller,
965 processor or consumer health data controller disclosed such personal
966 data, the disclosing controller, processor or consumer health data
967 controller did not have actual knowledge that the receiving processor or
968 third-party controller would violate said sections. A third-party
969 controller or processor receiving personal data from a controller,
970 processor or consumer health data controller in compliance with
971 sections 42-515 to 42-526, inclusive, as amended by this act, is likewise
972 not in violation of said sections for the transgressions of the controller,
973 processor or consumer health data controller from which such third-
974 party controller or processor receives such personal data.

975 Sec. 10. Subsections (a) and (b) of section 42-528 of the general statutes
976 are repealed and the following is substituted in lieu thereof (*Effective*
977 *October 1, 2025*):

978 (a) For the purposes of this section:

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

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

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

988 (4) "Personal data" has the same meaning as provided in section 42-
989 515, as amended by this act;

990 (5) "Social media platform" (A) means a public or semi-public
991 Internet-based service or application that (i) is used by a consumer in
992 this state, (ii) is primarily intended to connect and allow users to socially
993 interact within such service or application, and (iii) enables a user to (I)
994 construct a public or semi-public profile for the purposes of signing into
995 and using such service or application, (II) populate a public list of other
996 users with whom the user shares a social connection within such service
997 or application, and (III) create or post content that is viewable by other
998 users, including, but not limited to, on message boards, in chat rooms,
999 or through a landing page or main feed that presents the user with
1000 content generated by other users, and (B) does not include a public or
1001 semi-public Internet-based service or application that (i) exclusively
1002 provides electronic mail or direct messaging services, (ii) primarily
1003 consists of news, sports, entertainment, interactive video games,
1004 electronic commerce or content that is preselected by the provider or for
1005 which any chat, comments or interactive functionality is incidental to,
1006 directly related to, or dependent on the provision of such content, or (iii)
1007 is used by and under the direction of an educational entity, including,
1008 but not limited to, a learning management system or a student

1009 engagement program; and

1010 (6) "Unpublish" means to remove a social media platform account
1011 from public visibility.

1012 (b) (1) Not later than fifteen business days after a social media
1013 platform receives a request from a minor or, if the minor is younger than
1014 sixteen years of age, from such minor's parent or legal guardian to
1015 unpublish such minor's social media platform account, the social media
1016 platform shall unpublish such minor's social media platform account.

1017 (2) Not later than forty-five business days after a social media
1018 platform receives a request from a minor or, if the minor is younger than
1019 sixteen years of age, from such minor's parent or legal guardian to delete
1020 such minor's social media platform account, the social media platform
1021 shall delete such minor's social media platform account and cease
1022 processing such minor's personal data except where the preservation of
1023 such minor's social media platform account or personal data is
1024 otherwise permitted or required by applicable law, including, but not
1025 limited to, sections 42-515 to 42-525, inclusive, as amended by this act.
1026 A social media platform may extend such forty-five business day period
1027 by an additional forty-five business days if such extension is reasonably
1028 necessary considering the complexity and number of the consumer's
1029 requests, provided the social media platform informs the minor or, if the
1030 minor is younger than sixteen years of age, such minor's parent or legal
1031 guardian within the initial forty-five business day response period of
1032 such extension and the reason for such extension.

1033 (3) A social media platform shall establish, and shall describe in a
1034 privacy notice, one or more secure and reliable means for submitting a
1035 request pursuant to this subsection. A social media platform that
1036 provides a mechanism for a minor or, if the minor is younger than
1037 sixteen years of age, the minor's parent or legal guardian to initiate a
1038 process to delete or unpublish such minor's social media platform
1039 account shall be deemed to be in compliance with the provisions of this
1040 subsection.

1041 (4) No social media platform shall require a minor's parent or legal
1042 guardian to create a social media platform account to submit a request
1043 pursuant to this subsection. A social media platform may require a
1044 minor's parent or legal guardian to use an existing social media platform
1045 account to submit such a request, provided such parent or legal
1046 guardian has access to the existing social media platform account.

1047 Sec. 11. Section 42-529 of the general statutes is repealed and the
1048 following is substituted in lieu thereof (*Effective October 1, 2025*):

1049 For the purposes of this section and sections 42-529a to 42-529e,
1050 inclusive, as amended by this act:

1051 (1) "Adult" means any individual who is at least eighteen years of age;

1052 (2) "Consent" has the same meaning as provided in section 42-515, as
1053 amended by this act;

1054 (3) "Consumer" has the same meaning as provided in section 42-515,
1055 as amended by this act;

1056 (4) "Controller" has the same meaning as provided in section 42-515,
1057 as amended by this act;

1058 (5) "Heightened risk of harm to minors" means processing minors'
1059 personal data in a manner that presents any reasonably foreseeable risk
1060 of (A) any unfair or deceptive treatment of, or any unlawful disparate
1061 impact on, minors, (B) any material financial, physical or reputational
1062 injury to minors, [or] (C) any material physical or other intrusion upon
1063 the solitude or seclusion, or the private affairs or concerns, of minors if
1064 such intrusion would be offensive to a reasonable person, (D) any
1065 physical violence against minors, (E) any material harassment of minors
1066 on any online service, product or feature, which harassment is severe,
1067 pervasive or objectively offensive to a reasonable person, or (F) any
1068 sexual abuse or sexual exploitation of minors;

1069 (6) "HIPAA" has the same meaning as provided in section 42-515, as

1070 amended by this act;

1071 (7) "Minor" means any consumer who is younger than eighteen years
1072 of age;

1073 (8) "Online service, product or feature" means any service, product or
1074 feature that is provided online. "Online service, product or feature" does
1075 not include any (A) telecommunications service, as defined in 47 USC
1076 153, as amended from time to time, (B) broadband Internet access
1077 service, as defined in 47 CFR 54.400, as amended from time to time, or
1078 (C) delivery or use of a physical product;

1079 (9) "Person" has the same meaning as provided in section 42-515, as
1080 amended by this act;

1081 (10) "Personal data" has the same meaning as provided in section 42-
1082 515, as amended by this act;

1083 (11) "Precise geolocation data" has the same meaning as provided in
1084 section 42-515, as amended by this act;

1085 (12) "Process" and "processing" have the same meaning as provided
1086 in section 42-515, as amended by this act;

1087 (13) "Processor" has the same meaning as provided in section 42-515,
1088 as amended by this act;

1089 (14) "Profiling" has the same meaning as provided in section 42-515,
1090 as amended by this act;

1091 (15) "Protected health information" has the same meaning as
1092 provided in section 42-515, as amended by this act;

1093 (16) "Sale of personal data" has the same meaning as provided in
1094 section 42-515, as amended by this act;

1095 (17) "Targeted advertising" has the same meaning as provided in
1096 section 42-515, as amended by this act; and

1097 (18) "Third party" has the same meaning as provided in section 42-
1098 515, as amended by this act.

1099 Sec. 12. Section 42-529a of the general statutes is repealed and the
1100 following is substituted in lieu thereof (*Effective October 1, 2025*):

1101 (a) Each controller that offers any online service, product or feature
1102 to consumers whom such controller has actual knowledge, or [wilfully
1103 disregards] knowledge fairly implied on the basis of objective
1104 circumstances, are minors shall use reasonable care to avoid any
1105 heightened risk of harm to minors caused by such online service,
1106 product or feature. In any enforcement action brought by the Attorney
1107 General pursuant to section 42-529e, there shall be a rebuttable
1108 presumption that a controller used reasonable care as required under
1109 this section if the controller complied with the provisions of section 42-
1110 529b, as amended by this act, concerning data protection assessments
1111 and impact assessments.

1112 (b) (1) [Subject to the consent requirement established in subdivision
1113 (3) of this subsection, no] No controller that offers any online service,
1114 product or feature to consumers whom such controller has actual
1115 knowledge, or [wilfully disregards] knowledge fairly implied on the
1116 basis of objective circumstances, are minors shall [: (A) Process] process
1117 any minor's personal data; [(i) for] (A) For the purposes of [(I)] (i)
1118 targeted advertising, [(II)] or (ii) any sale of personal data; [, or (III)]
1119 profiling in furtherance of any fully automated decision made by such
1120 controller that produces any legal or similarly significant effect
1121 concerning the provision or denial by such controller of any financial or
1122 lending services, housing, insurance, education enrollment or
1123 opportunity, criminal justice, employment opportunity, health care
1124 services or access to essential goods or services, (ii)] (B) unless such
1125 processing is reasonably necessary to provide such online service,
1126 product or feature; [, (iii)] (C) for any processing purpose [(I)] (i) other
1127 than the processing purpose that the controller disclosed at the time
1128 such controller collected such personal data, or [(II)] (ii) that is
1129 reasonably necessary for, and compatible with, the processing purpose

1130 described in subparagraph [(A)(iii)(I)] (C)(i) of this subdivision; [,] or
1131 [(iv)] (D) for longer than is reasonably necessary to provide such online
1132 service, product or feature. [,] or (B) use any system design feature to
1133 significantly increase, sustain or extend any minor's use of such online
1134 service, product or feature.] The provisions of this subdivision shall not
1135 apply to any service or application that is used by and under the
1136 direction of an educational entity, including, but not limited to, a
1137 learning management system or a student engagement program.

1138 (2) [Subject to the consent requirement established in subdivision (3)
1139 of this subsection, no] No controller that offers an online service,
1140 product or feature to consumers whom such controller has actual
1141 knowledge, or [wilfully disregards] knowledge fairly implied on the
1142 basis of objective circumstances, are minors shall collect a minor's
1143 precise geolocation data unless: (A) Such precise geolocation data [is
1144 reasonably] are strictly necessary for the controller to provide such
1145 online service, product or feature and, if such data [is] are necessary to
1146 provide such online service, product or feature, such controller may
1147 only collect such data for the time necessary to provide such online
1148 service, product or feature; and (B) the controller provides to the minor
1149 a signal indicating that such controller is collecting such precise
1150 geolocation data, which signal shall be available to such minor for the
1151 entire duration of such collection.

1152 (3) (A) Subject to the consent requirement established in
1153 subparagraph (B) of this subdivision, no controller that offers any online
1154 service, product or feature to consumers whom such controller has
1155 actual knowledge, or knowledge fairly implied based on objective
1156 circumstances, are minors shall process any minor's personal data for
1157 purposes of profiling in furtherance of any automated decision made by
1158 such controller that produces any legal or similarly significant effect
1159 concerning the provision or denial by such controller of any financial or
1160 lending service, housing, insurance, education enrollment or
1161 opportunity, criminal justice, employment opportunity, health care
1162 service or access to any essential good or service, unless such processing

1163 is reasonably necessary to provide such online service, product or
1164 feature.

1165 [(3)] (B) No controller shall engage in the activities described in
1166 [subdivisions (1) and (2) of this subsection] subparagraph (A) of this
1167 subdivision unless the controller obtains the minor's consent or, if the
1168 minor is younger than thirteen years of age, the consent of such minor's
1169 parent or legal guardian. A controller that complies with the verifiable
1170 parental consent requirements established in the Children's Online
1171 Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations,
1172 rules, guidance and exemptions adopted pursuant to said act, as said act
1173 and such regulations, rules, guidance and exemptions may be amended
1174 from time to time, shall be deemed to have satisfied any requirement to
1175 obtain parental consent under this [subdivision] subparagraph.

1176 (c) (1) No controller that offers any online service, product or feature
1177 to consumers whom such controller has actual knowledge, or [wilfully
1178 disregards] knowledge fairly implied on the basis of objective
1179 circumstances, are minors shall: (A) Provide any consent mechanism
1180 that is designed to substantially subvert or impair, or is manipulated
1181 with the effect of substantially subverting or impairing, user autonomy,
1182 decision-making or choice; [or] (B) except as provided in subdivision (2)
1183 of this subsection, offer any direct messaging apparatus for use by
1184 minors [without providing] unless (i) such controller provides readily
1185 accessible and easy-to-use safeguards to [limit the ability of adults to
1186 send] enable any minor, or any minor's parent or legal guardian, to
1187 prevent any adult from sending any unsolicited [communications to
1188 minors with whom they are not connected] communication to such
1189 minor unless such minor and adult are already connected on such online
1190 service, product or feature, and (ii) the safeguards required under
1191 subparagraph (B)(i) of this subdivision, as a default setting, prevent any
1192 adult from sending any unsolicited communication to any minor unless
1193 such minor and adult are already connected on such online service,
1194 product or feature; or (C) except as provided in subdivision (3) of this
1195 subsection, use any system design feature to significantly increase,

1196 sustain or extend any minor's use of such online service, product or
1197 feature.

1198 (2) The provisions of subparagraph (B) of subdivision (1) of this
1199 subsection shall not apply to services where the predominant or
1200 exclusive function is: (A) Electronic mail; or (B) direct messaging
1201 consisting of text, photos or videos that are sent between devices by
1202 electronic means, where messages are (i) shared between the sender and
1203 the recipient, (ii) only visible to the sender and the recipient, and (iii) not
1204 posted publicly.

1205 (3) The provisions of subparagraph (C) of subdivision (1) of this
1206 subsection shall not apply to any service or application that is used by
1207 and under the direction of an educational entity, including, but not
1208 limited to, a learning management system or a student engagement
1209 program.

1210 Sec. 13. Section 42-529b of the general statutes is repealed and the
1211 following is substituted in lieu thereof (*Effective October 1, 2025*):

1212 (a) Each controller that [, on or after October 1, 2024,] offers any online
1213 service, product or feature to consumers whom such controller has
1214 actual knowledge, or [wilfully disregards] knowledge fairly implied
1215 based on objective circumstances, are minors shall conduct a data
1216 protection assessment for such online service, product or feature: (1) In
1217 a manner that is consistent with the requirements established in section
1218 42-522, as amended by this act; and (2) that addresses (A) the purpose
1219 of such online service, product or feature, (B) the categories of minors'
1220 personal data that such online service, product or feature processes, (C)
1221 the purposes for which such controller processes minors' personal data
1222 with respect to such online service, product or feature, and (D) any
1223 heightened risk of harm to minors that is a reasonably foreseeable result
1224 of offering such online service, product or feature to minors.

1225 (b) Each controller that offers any online service, product or feature
1226 to consumers whom such controller has actual knowledge, or

1227 knowledge fairly implied based on objective circumstances, are minors
1228 shall, if such online service, product or feature engages in any profiling
1229 based on such consumers' personal data, conduct an impact assessment
1230 for such online service, product or feature. Such impact assessment shall
1231 include, to the extent reasonably known by or available to the controller,
1232 as applicable: (1) A statement by the controller disclosing the purpose,
1233 intended use cases and deployment context of, and benefits afforded by,
1234 such online service, product or feature, if such online service, product
1235 or feature engages in any profiling for the purpose of making decisions
1236 that produce legal or similarly significant effects concerning such
1237 consumers; (2) an analysis of whether such profiling poses any
1238 reasonably foreseeable heightened risk of harm to minors and, if so, (A)
1239 the nature of such heightened risk of harm to minors, and (B) the steps
1240 that have been taken to mitigate such heightened risk of harm to minors;
1241 (3) a description of (A) the categories of personal data such online
1242 service, product or feature processes as inputs for the purposes of such
1243 profiling, and (B) the outputs such online service, product or feature
1244 produces for the purposes of such profiling; (4) an overview of the
1245 categories of personal data the controller used to customize such online
1246 service, product or feature for the purposes of such profiling, if the
1247 controller used data to customize such online service, product or feature
1248 for the purposes of such profiling; (5) a description of any transparency
1249 measures taken concerning such online service, product or feature with
1250 respect to such profiling, including, but not limited to, any measures
1251 taken to disclose to consumers that such online service, product or
1252 feature is being used for such profiling while such online service,
1253 product or feature is being used for such profiling; and (6) a description
1254 of the post-deployment monitoring and user safeguards provided
1255 concerning such online service, product or feature for the purposes of
1256 such profiling, including, but not limited to, the oversight, use and
1257 learning processes established by the controller to address issues arising
1258 from deployment of such online service, product or feature for the
1259 purposes of such profiling.

1260 [(b)] (c) Each controller that conducts a data protection assessment

1261 pursuant to subsection (a) of this section, or an impact assessment
1262 pursuant to subsection (b) of this section, shall: (1) Review such data
1263 protection assessment or impact assessment as necessary to account for
1264 any material change to the processing or profiling operations of the
1265 online service, product or feature that is the subject of such data
1266 protection assessment or impact assessment; and (2) maintain
1267 documentation concerning such data protection assessment or impact
1268 assessment for the longer of (A) the three-year period beginning on the
1269 date on which such processing or profiling operations cease, or (B) as
1270 long as such controller offers such online service, product or feature.

1271 [(c)] (d) A single data protection assessment or impact assessment
1272 may address a comparable set of processing or profiling operations that
1273 include similar activities.

1274 [(d)] (e) If a controller conducts a data protection assessment or
1275 impact assessment for the purpose of complying with another
1276 applicable law or regulation, the data protection assessment or impact
1277 assessment shall be deemed to satisfy the requirements established in
1278 this section if such data protection assessment or impact assessment is
1279 reasonably similar in scope and effect to the data protection assessment
1280 or impact assessment that would otherwise be conducted pursuant to
1281 this section.

1282 [(e)] (f) If any controller conducts a data protection assessment
1283 pursuant to subsection (a) of this section, or an impact assessment
1284 pursuant to subsection (b) of this section, and determines that the online
1285 service, product or feature that is the subject of such assessment poses a
1286 heightened risk of harm to minors, such controller shall establish and
1287 implement a plan to mitigate or eliminate such risk. The Attorney
1288 General may require a controller to disclose to the Attorney General a
1289 plan established pursuant to this subsection if the plan is relevant to an
1290 investigation conducted by the Attorney General. The controller shall
1291 disclose such plan to the Attorney General not later than ninety days
1292 after the Attorney General notifies the controller, in a form and manner
1293 prescribed by the Attorney General, that the Attorney General requires

1294 the controller to disclose such plan to the Attorney General.

1295 ~~[(f)]~~ (g) Data protection assessments, impact assessments and harm
1296 mitigation or elimination plans shall be confidential and shall be exempt
1297 from disclosure under the Freedom of Information Act, as defined in
1298 section 1-200. To the extent any information contained in a data
1299 protection assessment, impact assessment or harm mitigation or
1300 elimination plan disclosed to the Attorney General includes information
1301 subject to the attorney-client privilege or work product protection, such
1302 disclosure shall not constitute a waiver of such privilege or protection.

1303 Sec. 14. Section 42-529c of the general statutes is repealed and the
1304 following is substituted in lieu thereof (*Effective October 1, 2025*):

1305 (a) A processor shall adhere to the instructions of a controller, and
1306 shall: (1) Assist the controller in meeting the controller's obligations
1307 under sections 42-529 to 42-529e, inclusive, as amended by this act,
1308 taking into account (A) the nature of the processing, (B) the information
1309 available to the processor by appropriate technical and organizational
1310 measures, and (C) whether such assistance is reasonably practicable and
1311 necessary to assist the controller in meeting such obligations; and (2)
1312 provide any information that is necessary to enable the controller to
1313 conduct and document data protection assessments and impact
1314 assessments pursuant to section 42-529b, as amended by this act.

1315 (b) Each processor that offers any online service, product or feature
1316 to consumers whom such processor has actual knowledge, or
1317 knowledge fairly implied based on objective circumstances, are minors
1318 shall, if such online service, product or feature engages in any profiling
1319 based on such consumers' personal data, conduct an impact assessment
1320 for such online service, product or feature. Such impact assessment shall
1321 include, to the extent reasonably known by or available to the processor,
1322 as applicable: (1) A statement by the processor disclosing the purpose,
1323 intended use cases and deployment context of, and benefits afforded by,
1324 such online service, product or feature, if such online service, product
1325 or feature engages in any profiling for the purpose of making decisions

1326 that produce legal or similarly significant effects concerning such
1327 consumers; (2) an analysis of whether such profiling poses any
1328 reasonably foreseeable heightened risk of harm to minors and, if so, (A)
1329 the nature of such heightened risk of harm to minors, and (B) the steps
1330 that have been taken to mitigate such heightened risk of harm to minors;
1331 (3) a description of (A) the categories of personal data such online
1332 service, product or feature processes as inputs for the purposes of such
1333 profiling, and (B) the outputs such online service, product or feature
1334 produces for the purposes of such profiling; (4) an overview of the
1335 categories of personal data the processor used to customize such online
1336 service, product or feature for the purposes of such profiling, if the
1337 processor used data to customize such online service, product or feature
1338 for the purposes of such profiling; (5) a description of any transparency
1339 measures taken concerning such online service, product or feature with
1340 respect to such profiling, including, but not limited to, any measures
1341 taken to disclose to consumers that such online service, product or
1342 feature is being used for such profiling while such online service,
1343 product or feature is being used for such profiling; and (6) a description
1344 of the post-deployment monitoring and user safeguards provided
1345 concerning such online service, product or feature for the purposes of
1346 such profiling, including, but not limited to, the oversight, use and
1347 learning processes established by the processor to address issues arising
1348 from deployment of such online service, product or feature for the
1349 purposes of such profiling.

1350 (c) Each processor that conducts an impact assessment pursuant to
1351 subsection (b) of this section shall: (1) Review such impact assessment
1352 as necessary to account for any material change to the profiling
1353 operations of the online service, product or feature that is the subject of
1354 such impact assessment; and (2) maintain documentation concerning
1355 such impact assessment for the longer of (A) the three-year period
1356 beginning on the date on which such profiling operations cease, or (B)
1357 as long as such processor offers such online service, product or feature.

1358 (d) A single impact assessment may address a comparable set of

1359 profiling operations that include similar activities.

1360 (e) If a processor conducts an impact assessment for the purpose of
1361 complying with another applicable law or regulation, the impact
1362 assessment shall be deemed to satisfy the requirements established in
1363 this section if such impact assessment is reasonably similar in scope and
1364 effect to the impact assessment that would otherwise be conducted
1365 pursuant to this section.

1366 (f) If any processor conducts an impact assessment pursuant to
1367 subsection (b) of this section and determines that the online service,
1368 product or feature that is the subject of such assessment poses a
1369 heightened risk of harm to minors, such processor shall establish and
1370 implement a plan to mitigate or eliminate such risk. The Attorney
1371 General may require a processor to disclose to the Attorney General a
1372 plan established and implemented pursuant to this subsection if the
1373 plan is relevant to an investigation conducted by the Attorney General.

1374 (g) Impact assessments shall be confidential and shall be exempt from
1375 disclosure under the Freedom of Information Act, as defined in section
1376 1-200. To the extent any information contained in an impact assessment
1377 disclosed to the Attorney General includes information subject to the
1378 attorney-client privilege or work product protection, such disclosure
1379 shall not constitute a waiver of such privilege or protection.

1380 [(b)] (h) A contract between a controller and a processor shall satisfy
1381 the requirements established in subsection (b) of section 42-521, as
1382 amended by this act.

1383 [(c)] (i) Nothing in this section shall be construed to relieve a
1384 controller or processor from the liabilities imposed on the controller or
1385 processor by virtue of such controller's or processor's role in the
1386 processing relationship, as described in sections 42-529 to 42-529e,
1387 inclusive, as amended by this act.

1388 [(d)] (j) Determining whether a person is acting as a controller or
1389 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.

Sec. 15. Subsection (d) of section 42-529d of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(d) No obligation imposed on a controller or processor under any provision of sections 42-529 to 42-529c, inclusive, as amended by this act, 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 state-of-the-art security and privacy measures, including, but not limited to, pseudonymization,~~

1423 (D) subject to measures to ensure that such personal data are secure,
1424 protected and subject to suitable safeguards, including, but not limited
1425 to, strict controls concerning, and documentation of, access to such
1426 personal data, to avoid misuse and ensure that only authorized persons
1427 may access such personal data while preserving the confidentiality of
1428 such personal data, and (E) not transmitted, transferred or otherwise
1429 accessed by any third party; or [(4)] (5) perform solely internal
1430 operations that are (A) reasonably aligned with the expectations of a
1431 minor or reasonably anticipated based on the minor's existing
1432 relationship with the controller or processor, or (B) otherwise
1433 compatible with processing data in furtherance of the provision of a
1434 product or service specifically requested by a minor.

1435 Sec. 16. (NEW) (*Effective October 1, 2025*) (a) As used in this section:

1436 (1) "Brokered personal data" means any personal data that are
1437 categorized or organized for the purpose of enabling a data broker to
1438 sell or license such personal data to another person;

1439 (2) "Business" (A) means (i) a person who regularly engages in
1440 commercial activities for the purpose of generating income, (ii) a bank,
1441 Connecticut credit union, federal credit union, out-of-state bank, out-of-
1442 state trust company or out-of-state credit union, as said terms are
1443 defined in section 36a-2 of the general statutes, and (iii) any other person
1444 that controls, is controlled by or is under common control with a person
1445 described in subparagraph (A)(i) or (A)(ii) of this subdivision, and (B)
1446 does not include any body, authority, board, bureau, commission,
1447 district or agency of this state or of any political subdivision of this state;

1448 (3) "Consumer" has the same meaning as provided in section 42-515
1449 of the general statutes, as amended by this act;

1450 (4) "Data broker" means any business or, if such business is an entity,
1451 any portion of such business that sells or licenses brokered personal data
1452 to another person;

1453 (5) "Department" means the Department of Consumer Protection;

1454 (6) "License" (A) means to grant access to, or distribute, personal data
1455 in exchange for consideration, and (B) does not include any use of
1456 personal data for the sole benefit of the person who provided such
1457 personal data if such person maintains control over the use of such
1458 personal data;

1459 (7) "Person" has the same meaning as provided in section 42-515 of
1460 the general statutes, as amended by this act; and

1461 (8) "Personal data" (A) means any data concerning a consumer that,
1462 either alone or in combination with any other data that are sold or
1463 licensed by a data broker to another person, can reasonably be
1464 associated with the consumer, and (B) includes, but is not limited to, (i)
1465 a consumer's name or the name of any member of the consumer's
1466 immediate family or household, (ii) a consumer's address or the address
1467 of any member of the consumer's immediate family or household, (iii) a
1468 consumer's birth date or place of birth, (iv) the maiden name of a
1469 consumer's mother, (v) biometric data, as defined in section 42-515 of
1470 the general statutes, as amended by this act, concerning a consumer, and
1471 (vi) a consumer's Social Security number or any other government-
1472 issued identification number issued to the consumer.

1473 (b) (1) Except as provided in subdivision (4) of this subsection and
1474 subsection (d) of this section, no data broker shall sell or license
1475 brokered personal data in this state unless the data broker is actively
1476 registered with the Department of Consumer Protection in accordance
1477 with the provisions of this subsection. A data broker who desires to sell
1478 or license brokered personal data in this state shall submit an
1479 application to the department in a form and manner prescribed by the
1480 Commissioner of Consumer Protection. Each application for
1481 registration as a data broker shall be accompanied by a registration fee
1482 in the amount of six hundred dollars. Each registration issued pursuant
1483 to this subsection shall expire on December thirty-first of the year in
1484 which such registration was issued and may be renewed for successive
1485 one-year terms upon application made in the manner set forth in this
1486 subsection and payment of a registration renewal fee in the amount of

1487 six hundred dollars.

1488 (2) Except as provided in subdivision (4) of this subsection, each
1489 application submitted to the department pursuant to subdivision (1) of
1490 this subsection shall include:

1491 (A) The applicant's name, mailing address, electronic mail address
1492 and telephone number;

1493 (B) The address of the applicant's primary Internet web site; and

1494 (C) A statement by the applicant disclosing the measures the
1495 applicant shall take to ensure that no personal data are sold or licensed
1496 in violation of the provisions of sections 42-515 to 42-525, inclusive, of
1497 the general statutes, as amended by this act.

1498 (3) The department shall make all information that an applicant
1499 submits to the department pursuant to subdivision (2) of this subsection
1500 publicly available on the department's Internet web site.

1501 (4) The department may approve and renew an application for
1502 registration as a data broker in accordance with the terms of an
1503 agreement between the department and the Nationwide Multistate
1504 Licensing System.

1505 (c) No data broker shall sell or license any personal data in violation
1506 of the provisions of sections 42-515 to 42-525, inclusive, of the general
1507 statutes, as amended by this act. Each data broker shall implement
1508 measures to ensure that the data broker does not sell or license any
1509 personal data in violation of the provisions of sections 42-515 to 42-525,
1510 inclusive, of the general statutes, as amended by this act.

1511 (d) (1) The provisions of this section shall not apply to: (A) A
1512 consumer reporting agency, as defined in 15 USC 1681a(f), as amended
1513 from time to time, a person that furnishes information to a consumer
1514 reporting agency, as provided in 15 USC 1681s-2, as amended from time
1515 to time, or a user of a consumer report, as defined in 15 USC 1681a(d),

1516 as amended from time to time, to the extent that the consumer reporting
1517 agency, person or user engages in activities that are subject to regulation
1518 under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended
1519 from time to time; (B) a financial institution, an affiliate or a nonaffiliated
1520 third party, as said terms are defined in 15 USC 6809, as amended from
1521 time to time, to the extent that the financial institution, affiliate or
1522 nonaffiliated third party engages in activities that are subject to
1523 regulation under Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et
1524 seq., and the regulations adopted thereunder, as said act and regulations
1525 may be amended from time to time; (C) a business that collects
1526 information concerning a consumer if the consumer (i) is a customer,
1527 subscriber or user of goods or services sold or offered by the business,
1528 (ii) is in a contractual relationship with the business, (iii) is an investor
1529 in the business, (iv) is a donor to the business, or (v) otherwise maintains
1530 a relationship with the business that is similar to the relationships
1531 described in subparagraphs (C)(i) to (C)(iv), inclusive, of this
1532 subdivision; or (D) a business that performs services for, or acts as an
1533 agent or on behalf of, a business described in subparagraph (C) of this
1534 subdivision.

1535 (2) No provision of this section shall be construed to prohibit an
1536 unregistered data broker from engaging in any sale or licensing of
1537 brokered personal data if such sale or licensing exclusively involves: (A)
1538 Publicly available information (i) concerning a consumer's business or
1539 profession, or (ii) sold or licensed as part of a service that provides alerts
1540 for health or safety purposes; (B) information that is lawfully available
1541 from any federal, state or local government record; (C) providing digital
1542 access to any (i) journal, book, periodical, newspaper, magazine or news
1543 media, or (ii) educational, academic or instructional work; (D)
1544 developing or maintaining an electronic commerce service or software;
1545 (E) providing directory assistance or directory information services as,
1546 or on behalf of, a telecommunications carrier; or (F) a one-time or
1547 occasional disposition of the assets of a business, or any portion of a
1548 business, as part of a transfer of control over the assets of the business
1549 that is not part of the ordinary conduct of such business or portion of

1550 such business.

1551 (e) The Commissioner of Consumer Protection may adopt
1552 regulations, in accordance with the provisions of chapter 54 of the
1553 general statutes, to implement the provisions of this section.

1554 (f) The Commissioner of Consumer Protection, after providing notice
1555 and conducting a hearing in accordance with the provisions of chapter
1556 54 of the general statutes, may impose a civil penalty of not more than
1557 five hundred dollars per day for each violation of subsections (b) to (d),
1558 inclusive, of this section. The sum of civil penalties imposed on a data
1559 broker pursuant to this subsection shall not exceed ten thousand dollars
1560 during any calendar year.

1561 Sec. 17. (NEW) (*Effective January 1, 2026*) (a) As used in this section:

1562 (1) "Abuser" means an individual who (A) is identified by a survivor
1563 pursuant to subsection (b) of this section, and (B) has committed, or
1564 allegedly committed, a covered act against the survivor making the
1565 connected vehicle services request;

1566 (2) "Account holder" means an individual who is (A) a party to a
1567 contract with a covered provider that involves a connected vehicle
1568 service, or (B) a subscriber, customer or registered user of a connected
1569 vehicle service;

1570 (3) "Connected vehicle service" means any capability provided by or
1571 on behalf of a motor vehicle manufacturer that enables a person to
1572 remotely obtain data from, or send commands to, a covered vehicle,
1573 including, but not limited to, any such capability provided by way of a
1574 software application that is designed to be operated on a mobile device;

1575 (4) "Connected vehicle service request" means a request by a survivor
1576 to terminate or disable an abuser's access to a connected vehicle service;

1577 (5) "Covered act" means conduct that constitutes (A) a crime
1578 described in Section 40002(a) of the Violence Against Women Act of

1579 1994, 34 USC 12291(a), as amended from time to time, (B) an act or
1580 practice described in 22 USC 7102(11) or (12), as amended from time to
1581 time, or (C) a crime, act or practice that is (i) similar to a crime, act or
1582 practice described in subparagraph (A) or (B) of this subdivision, and
1583 (ii) prohibited under federal, state or tribal law;

1584 (6) "Covered connected vehicle services account" means an account
1585 or other means by which a person enrolls in, or obtains access to, a
1586 connected vehicle service;

1587 (7) "Covered provider" means a motor vehicle manufacturer, or an
1588 entity acting on behalf of a motor vehicle manufacturer, that provides a
1589 connected vehicle service;

1590 (8) "Covered vehicle" means a motor vehicle that is (A) the subject of
1591 a connected vehicle request, and (B) identified by a survivor pursuant
1592 to subsection (b) of this section;

1593 (9) "Emergency situation" means a situation that, if allowed to
1594 continue, poses an imminent risk of death or serious bodily harm;

1595 (10) "In-vehicle interface" means a feature or mechanism installed in
1596 a motor vehicle that allows an individual within the motor vehicle to
1597 terminate or disable connected vehicle services;

1598 (11) "Person" means an individual, association, company, limited
1599 liability company, corporation, partnership, sole proprietorship, trust or
1600 other legal entity; and

1601 (12) "Survivor" means an individual (A) who is eighteen years of age
1602 or older, and (B) against whom a covered act has been committed or
1603 allegedly committed.

1604 (b) A survivor may submit a connected vehicle service request to a
1605 covered provider pursuant to this subsection. Each connected vehicle
1606 service request submitted pursuant to this subsection shall, at a
1607 minimum, include (1) the vehicle identification number of the covered

1608 vehicle, (2) the name of the abuser, and (3) (A) proof that the survivor is
1609 the sole owner of the covered vehicle, (B) if the survivor is not the sole
1610 owner of the covered vehicle, proof that the survivor is legally entitled
1611 to exclusive possession of the covered vehicle, which proof may take the
1612 form of a court order awarding exclusive possession of the covered
1613 vehicle to the survivor, or (C) if the abuser owns the covered vehicle, in
1614 whole or in part, a dissolution of marriage decree, restraining order or
1615 temporary restraining order (i) naming the abuser, and (ii) (I) granting
1616 exclusive possession of the covered vehicle to the survivor, or (II)
1617 restricting the abuser's use of a connected vehicle service against the
1618 survivor.

1619 (c) (1) Not later than two business days after a survivor submits a
1620 connected vehicle service request to a covered provider pursuant to
1621 subsection (b) of this section, the covered provider shall take one or
1622 more of the following actions requested by the survivor in the connected
1623 vehicle service request, regardless of whether the abuser identified in
1624 the connected vehicle service request is an account holder: (A)
1625 Terminate or disable the covered connected vehicle services account
1626 associated with such abuser; (B) (i) terminate or disable the covered
1627 connected vehicle services account associated with the covered vehicle,
1628 including, but not limited to, by resetting or deleting any data or
1629 wireless connection with respect to the covered vehicle, and (ii) provide
1630 instructions to the survivor on how to reestablish a covered connected
1631 vehicle services account; (C) (i) terminate or disable covered connected
1632 vehicle services for the covered vehicle, including, but not limited to, by
1633 resetting or deleting any data or wireless connection with respect to the
1634 covered vehicle, and (ii) provide instructions to the survivor on how to
1635 reestablish connected vehicle services; or (D) if the motor vehicle has an
1636 in-vehicle interface, provide information to the survivor concerning (i)
1637 the availability of the in-vehicle interface, and (ii) how to terminate or
1638 disable connected vehicle services using the in-vehicle interface.

1639 (2) After the covered provider has taken action pursuant to
1640 subdivision (1) of this subsection, the covered provider shall deny any

1641 request made by the abuser to obtain any data that (A) were generated
1642 by the connected vehicle service after the abuser's access to such
1643 connected vehicle service was terminated or disabled in response to the
1644 connected vehicle service request, and (B) are maintained by the covered
1645 provider.

1646 (3) The covered provider shall not refuse to take action pursuant to
1647 subdivision (1) of this subsection on the basis that any requirement,
1648 other than a requirement established in subsection (b) of this section, has
1649 not been satisfied, including, but not limited to, any requirement that
1650 provides for (A) payment of any fee, penalty or other charge, (B)
1651 maintaining or extending the term of the covered connected vehicle
1652 services account, (C) obtaining approval from any account holder other
1653 than the survivor, or (D) increasing the rate charged for the connected
1654 vehicle service.

1655 (4) (A) If the covered provider intends to provide any formal notice
1656 to the abuser regarding any action set forth in subdivision (1) of this
1657 subsection, the covered provider shall first notify the survivor of the
1658 date on which the covered provider intends to provide such notice to
1659 the abuser.

1660 (B) The covered provider shall take reasonable steps to ensure that
1661 the covered provider only provides formal notice to the abuser,
1662 pursuant to subparagraph (A) of this subdivision, (i) at least three days
1663 after the covered provider notified the survivor pursuant to
1664 subparagraph (A) of this subdivision, and (ii) after the covered provider
1665 has terminated or disabled the abuser's access to the connected vehicle
1666 service.

1667 (5) (A) The covered provider shall not be required to take any action
1668 pursuant to subdivision (1) of this subsection if the covered provider
1669 cannot operationally or technically effectuate such action.

1670 (B) If the covered provider cannot operationally or technically
1671 effectuate any action as set forth in subparagraph (A) of this subdivision,

1672 the covered provider shall promptly notify the survivor who submitted
1673 the connected vehicle service request that the covered provider cannot
1674 operationally or technically effectuate such action, which notice shall, at
1675 a minimum, disclose whether the covered provider's inability to
1676 operationally or technically effectuate such action can be remedied and,
1677 if so, any steps the survivor can take to assist the covered provider in
1678 remedying such inability.

1679 (d) (1) The covered provider and each officer, director, employee,
1680 vendor or agent of the covered provider shall treat all information
1681 submitted by the survivor under subsection (b) of this section as
1682 confidential, and shall securely dispose of such information not later
1683 than ninety days after the survivor submitted such information.

1684 (2) The covered provider shall not disclose any information
1685 submitted by the survivor under subsection (b) of this section to a third
1686 party unless (A) the covered provider has obtained affirmative consent
1687 from the survivor to disclose such information to the third party, or (B)
1688 disclosing such information to the third party is necessary to effectuate
1689 the connected vehicle service request.

1690 (3) Nothing in subdivision (1) of this subsection shall be construed to
1691 prohibit the covered provider from maintaining, for longer than the
1692 period specified in subdivision (1) of this subsection, a record that
1693 verifies that the survivor fulfilled the conditions of the connected vehicle
1694 service request as set forth in subsection (b) of this section, provided
1695 such record is limited to what is reasonably necessary and proportionate
1696 to verify that the survivor fulfilled such conditions.

1697 (e) The survivor shall take reasonable steps to notify the covered
1698 provider of any change in the ownership or possession of the covered
1699 vehicle that materially affects the need for the covered provider to take
1700 action pursuant to subdivision (1) of subsection (c) of this section.

1701 (f) The requirements established in this section shall not prohibit or
1702 prevent a covered provider from terminating or disabling an abuser's

1703 access to a connected vehicle service in an emergency situation after
 1704 receiving a connected vehicle service request.

1705 (g) Each covered provider shall publicly post, on such covered
 1706 provider's Internet web site, a statement describing how a survivor may
 1707 submit a connected vehicle service request to such covered provider.

1708 (h) Each covered provider and each officer, director, employee,
 1709 vendor or agent of a covered provider shall be immune from any civil
 1710 liability which might otherwise arise from any act or omission
 1711 committed by such covered provider, officer, director, employee,
 1712 vendor or agent pursuant to subsections (a) to (g), inclusive, of this
 1713 section, provided such act or omission was committed in compliance
 1714 with the provisions of said subsections."

This act shall take effect as follows and shall amend the following sections:

Section 1	<i>October 1, 2025</i>	New section
Sec. 2	<i>October 1, 2025</i>	42-515
Sec. 3	<i>October 1, 2025</i>	42-516
Sec. 4	<i>October 1, 2025</i>	42-517(a) and (b)
Sec. 5	<i>October 1, 2025</i>	42-518
Sec. 6	<i>October 1, 2025</i>	42-520
Sec. 7	<i>October 1, 2025</i>	42-521
Sec. 8	<i>October 1, 2025</i>	42-522
Sec. 9	<i>October 1, 2025</i>	42-524(a) to (d)
Sec. 10	<i>October 1, 2025</i>	42-528(a) and (b)
Sec. 11	<i>October 1, 2025</i>	42-529
Sec. 12	<i>October 1, 2025</i>	42-529a
Sec. 13	<i>October 1, 2025</i>	42-529b
Sec. 14	<i>October 1, 2025</i>	42-529c
Sec. 15	<i>October 1, 2025</i>	42-529d(d)
Sec. 16	<i>October 1, 2025</i>	New section
Sec. 17	<i>January 1, 2026</i>	New section