



General Assembly

**Amendment**

January Session, 2025

LCO No. 8278



Offered by:

SEN. MARONEY, 14<sup>th</sup> Dist.

REP. LEMAR, 96<sup>th</sup> Dist.

REP. TURCO, 27<sup>th</sup> 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 February 1, 2026*):

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 February 1, 2026*):

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 *February 1, 2026*):

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; (9)  
312 bank, Connecticut credit union, federal credit union, out-of-state bank  
313 or out-of-state credit union, or any affiliate or subsidiary thereof, as such  
314 terms are defined in section 36a-2, that is regulated by the Department  
315 of Banking and in compliance with all applicable requirements  
316 established by the Banking Commissioner concerning personal data; or  
317 (10) agent, broker-dealer, investment adviser or investment adviser  
318 agent, as such terms are defined in section 36b-3, who is regulated by

319 the Department of Banking or the Securities and Exchange Commission  
320 and is in compliance with all applicable requirements established by the  
321 Banking Commissioner or the Securities and Exchange Commission  
322 concerning personal data.

323 (b) The following information and data [is] are exempt from the  
324 provisions of sections 42-515 to 42-526, inclusive, as amended by this  
325 act: (1) Protected health information under HIPAA; (2) patient-  
326 identifying information for purposes of 42 USC 290dd-2; (3) identifiable  
327 private information for purposes of the federal policy for the protection  
328 of human subjects under 45 CFR 46; (4) identifiable private information  
329 that is otherwise information collected as part of human subjects  
330 research pursuant to the good clinical practice guidelines issued by the  
331 International Council for Harmonization of Technical Requirements for  
332 Pharmaceuticals for Human Use; (5) personal data for purposes of the  
333 protection of human subjects under 21 CFR Parts 6, 50 and 56, or  
334 personal data used or shared in research, as defined in 45 CFR 164.501,  
335 that is conducted in accordance with the standards set forth in this  
336 subdivision and subdivisions (3) and (4) of this subsection, or other  
337 research conducted in accordance with applicable law; (6) information  
338 and documents created for purposes of the Health Care Quality  
339 Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work  
340 product for purposes of section 19a-127o and the Patient Safety and  
341 Quality Improvement Act, 42 USC 299b-21 et seq., as amended from  
342 time to time; (8) information derived from any of the health care-related  
343 information listed in this subsection that is de-identified in accordance  
344 with the requirements for de-identification pursuant to HIPAA; (9)  
345 information originating from and intermingled to be indistinguishable  
346 with, or information treated in the same manner as, information exempt  
347 under this subsection that is maintained by a covered entity or business  
348 associate, program or qualified service organization, as specified in 42  
349 USC 290dd-2, as amended from time to time; (10) information used for  
350 public health activities and purposes as authorized by HIPAA,  
351 community health activities and population health activities; (11) the  
352 collection, maintenance, disclosure, sale, communication or use of any

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

387 Sec. 5. Section 42-518 of the general statutes is repealed and the  
388 following is substituted in lieu thereof (*Effective February 1, 2026*):

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

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

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

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

449 (1) A controller shall respond to the consumer without undue delay,  
450 but not later than forty-five days after receipt of the request. The  
451 controller may extend the response period by forty-five additional days  
452 when reasonably necessary, considering the complexity and number of  
453 the consumer's requests, provided the controller informs the consumer

454 of any such extension within the initial forty-five-day response period  
455 and of the reason for the extension.

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

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

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



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

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

510 (e) A controller shall not disclose the following personal data in  
511 response to a request to exercise the consumer's rights under  
512 subdivision (1) of subsection (a) of this section, and shall instead inform  
513 the consumer or the person exercising such right on behalf of the  
514 consumer, with sufficient particularity, that the controller has collected  
515 such personal data: (1) The consumer's Social Security number; (2) the  
516 consumer's driver's license number, state identification card number or  
517 other government-issued identification number; (3) the consumer's  
518 financial account number; (4) the consumer's health insurance  
519 identification number or medical identification number; (5) the

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

522 Sec. 6. Section 42-520 of the general statutes is repealed and the  
523 following is substituted in lieu thereof (*Effective February 1, 2026*):

524 (a) ~~(1)~~ A controller shall: ~~[(1)]~~ (A) Limit the collection of personal data  
525 to what is [adequate, relevant and] reasonably necessary and  
526 proportionate in relation to the purposes for which such data [is] are  
527 processed, as disclosed to the consumer; [(2) except as otherwise  
528 provided in sections 42-515 to 42-525, inclusive] (B) unless the controller  
529 obtains the consumer's consent, not process the consumer's personal  
530 data for [purposes] any new purpose that [are] is neither reasonably  
531 necessary to, nor compatible with, the [disclosed] purposes [for which  
532 such personal data is processed, as] that were disclosed to the consumer  
533 [unless the controller obtains the consumer's consent; (3)] pursuant to  
534 subparagraph (A) of this subdivision, taking into account (i) the  
535 consumer's reasonable expectation regarding such personal data at the  
536 time such personal data were collected based on the purposes that were  
537 disclosed to the consumer pursuant to subparagraph (A) of this  
538 subdivision, (ii) the relationship that such new purpose bears to the  
539 purposes that were disclosed to the consumer pursuant to  
540 subparagraph (A) of this subdivision, (iii) the impact that processing  
541 such personal data for such new purpose might have on the consumer,  
542 (iv) the relationship between the consumer and the controller and the  
543 context in which the personal data were collected, and (v) the existence  
544 of additional safeguards, including, but not limited to, encryption or  
545 pseudonymization, in processing such personal data for such new  
546 purpose; (C) establish, implement and maintain reasonable  
547 administrative, technical and physical data security practices to protect  
548 the confidentiality, integrity and accessibility of personal data  
549 appropriate to the volume and nature of the personal data at issue; [(4)]  
550 (D) not process sensitive data concerning a consumer unless such  
551 processing is reasonably necessary in relation to the purposes for which  
552 such sensitive data are processed and without obtaining the consumer's

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

586 [(b)] (2) Nothing in subdivision (1) of this subsection [(a) of this

587 section] shall be construed to require a controller to provide a product  
588 or service that requires the personal data of a consumer which the  
589 controller does not collect or maintain, or prohibit a controller from  
590 offering a different price, rate, level, quality or selection of goods or  
591 services to a consumer, including offering goods or services for no fee,  
592 if the offering is in connection with a consumer's voluntary participation  
593 in a bona fide loyalty, rewards, premium features, discounts or club card  
594 program.

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

619 (2) A controller shall make the privacy notice required under

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

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

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

652 [(d) If a controller sells personal data to third parties or processes

653 personal data for targeted advertising, the controller shall clearly and  
654 conspicuously disclose such processing, as well as the manner in which  
655 a consumer may exercise the right to opt out of such processing.]

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

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

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

679 (I) Not unfairly disadvantage another controller;

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

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

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

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

692 (B) If a consumer's decision to opt out of any processing of the  
693 consumer's personal data for the purposes of targeted advertising, or  
694 any sale of such personal data, through an opt-out preference signal sent  
695 in accordance with the provisions of subparagraph (A) of this  
696 subdivision conflicts with the consumer's existing controller-specific  
697 privacy setting or voluntary participation in a controller's bona fide  
698 loyalty, rewards, premium features, discounts or club card program, the  
699 controller shall comply with such consumer's opt-out preference signal  
700 but may notify such consumer of such conflict and provide to such  
701 consumer the choice to confirm such controller-specific privacy setting  
702 or participation in such program.

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

709 Sec. 7. Section 42-521 of the general statutes is repealed and the  
710 following is substituted in lieu thereof (*Effective February 1, 2026*):

711 (a) A processor shall adhere to the instructions of a controller and  
712 shall assist the controller in meeting the controller's obligations under  
713 sections 42-515 to 42-525, inclusive, as amended by this act. Such  
714 assistance shall include: (1) Taking into account the nature of processing

715 and [the information available to the processor, by appropriate technical  
716 and organizational measures,] insofar as is [reasonably practicable]  
717 possible, to fulfill the controller's obligation to respond to [consumer  
718 rights requests] consumers' requests to exercise their rights under  
719 section 42-518, as amended by this act; (2) taking into account the nature  
720 of processing and the information available to the processor, by  
721 assisting the controller in meeting the controller's obligations in relation  
722 to the security of processing the personal data and in relation to the  
723 notification of a breach of security, as defined in section 36a-701b, of the  
724 system of the processor, in order to meet the controller's obligations; and  
725 (3) providing necessary information to enable the controller to conduct  
726 and document data protection assessments and impact assessments.

727 (b) A contract between a controller and a processor shall govern the  
728 processor's data processing procedures with respect to processing  
729 performed on behalf of the controller. The contract shall be binding and  
730 clearly set forth instructions for processing data, the nature and purpose  
731 of processing, the type of data subject to processing, the duration of  
732 processing and the rights and obligations of both parties. The contract  
733 shall also require that the processor: (1) Ensure that each person  
734 processing personal data is subject to a duty of confidentiality with  
735 respect to the data; (2) at the controller's direction, delete or return all  
736 personal data to the controller as requested at the end of the provision  
737 of services, unless retention of the personal data is required by law; (3)  
738 upon the reasonable request of the controller, make available to the  
739 controller all information in its possession necessary to demonstrate the  
740 processor's compliance with the obligations in sections 42-515 to 42-525,  
741 inclusive, as amended by this act; (4) after providing the controller an  
742 opportunity to object, engage any subcontractor pursuant to a written  
743 contract that requires the subcontractor to meet the obligations of the  
744 processor with respect to the personal data; and (5) allow, and cooperate  
745 with, reasonable assessments by the controller or the controller's  
746 designated assessor, or the processor may arrange for a qualified and  
747 independent assessor to conduct an assessment of the processor's  
748 policies and technical and organizational measures in support of the



749 obligations under sections 42-515 to 42-525, inclusive, as amended by  
750 this act, using an appropriate and accepted control standard or  
751 framework and assessment procedure for such assessments. The  
752 processor shall provide a report of such assessment to the controller  
753 upon request.

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

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

772 Sec. 8. Section 42-522 of the general statutes is repealed and the  
773 following is substituted in lieu thereof (*Effective February 1, 2026*):

774 (a) For the purposes of this section, processing that presents a  
775 heightened risk of harm to a consumer includes: (1) The processing of  
776 personal data for the purposes of targeted advertising; (2) the sale of  
777 personal data; (3) the processing of personal data for the purposes of  
778 profiling, where such profiling presents a reasonably foreseeable risk of  
779 (A) unfair or deceptive treatment of, or unlawful disparate impact on,  
780 consumers, (B) financial, physical or reputational injury to consumers,

781 (C) a physical or other intrusion upon the solitude or seclusion, or the  
782 private affairs or concerns, of consumers, where such intrusion would  
783 be offensive to a reasonable person, or (D) other substantial injury to  
784 consumers; and (4) the processing of sensitive data.

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

799       [(b) Data protection assessments] (2) Each data protection assessment  
800 conducted pursuant to subdivision (1) of this subsection [(a) of this  
801 section] shall identify and weigh the benefits that may flow, directly and  
802 indirectly, from the processing to the controller, the consumer, other  
803 stakeholders and the public against the potential risks to the rights of  
804 the consumer associated with such processing, as mitigated by  
805 safeguards that can be employed by the controller to reduce such risks.  
806 The controller shall factor into [any] each such data protection  
807 assessment the use of de-identified data and the reasonable expectations  
808 of consumers, as well as the context of the processing and the  
809 relationship between the controller and the consumer whose personal  
810 data will be processed.

811       (c) Each controller that engages in any profiling for the purposes of  
812 making a decision that produces any legal or similarly significant effect  
813 concerning a consumer shall conduct an impact assessment for such

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

836     [(c)] (d) The Attorney General may require that a controller disclose  
837 any data protection assessment or impact assessment that is relevant to  
838 an investigation conducted by the Attorney General, and the controller  
839 shall make the data protection assessment or impact assessment  
840 available to the Attorney General. The Attorney General may evaluate  
841 the data protection assessment or impact assessment for compliance  
842 with the responsibilities set forth in sections 42-515 to 42-525, inclusive,  
843 as amended by this act. Data protection assessments and impact  
844 assessments shall be confidential and shall be exempt from disclosure  
845 under the Freedom of Information Act, as defined in section 1-200. To  
846 the extent any information contained in a data protection assessment or  
847 impact assessment disclosed to the Attorney General includes

848 information subject to attorney-client privilege or work product  
849 protection, such disclosure shall not constitute a waiver of such  
850 privilege or protection.

851 ~~[(d)]~~ (e) A single data protection assessment or impact assessment  
852 may address a comparable set of processing operations that include  
853 similar activities.

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

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

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

867 Sec. 9. Subsections (a) to (d), inclusive, of section 42-524 of the general  
868 statutes are repealed and the following are substituted in lieu thereof  
869 (*Effective February 1, 2026*):

870 (a) Nothing in sections 42-515 to 42-526, inclusive, as amended by this  
871 act, shall be construed to restrict a controller's, processor's or consumer  
872 health data controller's ability to: (1) Comply with federal, state or  
873 municipal ordinances or regulations; (2) comply with a civil, criminal or  
874 regulatory inquiry, investigation, subpoena or summons by federal,  
875 state, municipal or other governmental authorities; (3) cooperate with  
876 law enforcement agencies concerning conduct or activity that the  
877 controller, processor or consumer health data controller reasonably and  
878 in good faith believes may violate federal, state or municipal ordinances

879 or regulations; (4) investigate, establish, exercise, prepare for or defend  
880 legal claims; (5) provide a product or service specifically requested by a  
881 consumer; (6) perform under a contract to which a consumer is a party,  
882 including fulfilling the terms of a written warranty; (7) take steps at the  
883 request of a consumer prior to entering into a contract; (8) take  
884 immediate steps to protect an interest that is essential for the life or  
885 physical safety of the consumer or another individual, and where the  
886 processing cannot be manifestly based on another legal basis; (9)  
887 prevent, detect, protect against or respond to security incidents, identity  
888 theft, fraud, harassment, malicious or deceptive activities or any illegal  
889 activity, preserve the integrity or security of systems or investigate,  
890 report or prosecute those responsible for any such action; (10) engage in  
891 public or peer-reviewed scientific or statistical research in the public  
892 interest that adheres to all other applicable ethics and privacy laws and  
893 is approved, monitored and governed by an institutional review board  
894 that determines, or similar independent oversight entities that  
895 determine, (A) whether the deletion of the information is likely to  
896 provide substantial benefits that do not exclusively accrue to the  
897 controller or consumer health data controller, (B) the expected benefits  
898 of the research outweigh the privacy risks, and (C) whether the  
899 controller or consumer health data controller has implemented  
900 reasonable safeguards to mitigate privacy risks associated with  
901 research, including any risks associated with re-identification; (11) assist  
902 another controller, processor, consumer health data controller or third  
903 party with any of the obligations under sections 42-515 to 42-526,  
904 inclusive, as amended by this act; or (12) process personal data for  
905 reasons of public interest in the area of public health, community health  
906 or population health, but solely to the extent that such processing is (A)  
907 subject to suitable and specific measures to safeguard the rights of the  
908 consumer whose personal data [is] are being processed, and (B) under  
909 the responsibility of a professional subject to confidentiality obligations  
910 under federal, state or local law.

911 (b) The obligations imposed on controllers, processors or consumer  
912 health data controllers under sections 42-515 to 42-526, inclusive, as

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

943 (c) The obligations imposed on controllers, processors or consumer  
944 health data controllers under sections 42-515 to 42-526, inclusive, as  
945 amended by this act, shall not apply where compliance by the controller,  
946 processor or consumer health data controller with said sections would

947 violate an evidentiary privilege under the laws of this state. Nothing in  
948 sections 42-515 to 42-526, inclusive, as amended by this act, shall be  
949 construed to prevent a controller, processor or consumer health data  
950 controller from providing personal data concerning a consumer to a  
951 person covered by an evidentiary privilege under the laws of the state  
952 as part of a privileged communication.

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

969 Sec. 10. Subsections (a) and (b) of section 42-528 of the general statutes  
970 are repealed and the following is substituted in lieu thereof (*Effective*  
971 *February 1, 2026*):

972 (a) For the purposes of this section:

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

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

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

982 (4) "Personal data" has the same meaning as provided in section 42-  
983 515, as amended by this act;

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

1004 (6) "Unpublish" means to remove a social media platform account  
1005 from public visibility.

1006 (b) (1) Not later than fifteen business days after a social media  
1007 platform receives a request from a minor or, if the minor is younger than  
1008 sixteen years of age, from such minor's parent or legal guardian to



1009 unpublish such minor's social media platform account, the social media  
1010 platform shall unpublish such minor's social media platform account.

1011 (2) Not later than forty-five business days after a social media  
1012 platform receives a request from a minor or, if the minor is younger than  
1013 sixteen years of age, from such minor's parent or legal guardian to delete  
1014 such minor's social media platform account, the social media platform  
1015 shall delete such minor's social media platform account and cease  
1016 processing such minor's personal data except where the preservation of  
1017 such minor's social media platform account or personal data is  
1018 otherwise permitted or required by applicable law, including, but not  
1019 limited to, sections 42-515 to 42-525, inclusive, as amended by this act.  
1020 A social media platform may extend such forty-five business day period  
1021 by an additional forty-five business days if such extension is reasonably  
1022 necessary considering the complexity and number of the consumer's  
1023 requests, provided the social media platform informs the minor or, if the  
1024 minor is younger than sixteen years of age, such minor's parent or legal  
1025 guardian within the initial forty-five business day response period of  
1026 such extension and the reason for such extension.

1027 (3) A social media platform shall establish, and shall describe in a  
1028 privacy notice, one or more secure and reliable means for submitting a  
1029 request pursuant to this subsection. A social media platform that  
1030 provides a mechanism for a minor or, if the minor is younger than  
1031 sixteen years of age, the minor's parent or legal guardian to initiate a  
1032 process to delete or unpublish such minor's social media platform  
1033 account shall be deemed to be in compliance with the provisions of this  
1034 subsection.

1035 (4) No social media platform shall require a minor's parent or legal  
1036 guardian to create a social media platform account to submit a request  
1037 pursuant to this subsection. A social media platform may require a  
1038 minor's parent or legal guardian to use an existing social media platform  
1039 account to submit such a request, provided such parent or legal  
1040 guardian has access to the existing social media platform account.

1041 Sec. 11. Section 42-529 of the general statutes is repealed and the  
1042 following is substituted in lieu thereof (*Effective February 1, 2026*):

1043 For the purposes of this section and sections 42-529a to 42-529e,  
1044 inclusive, as amended by this act:

1045 (1) "Adult" means any individual who is at least eighteen years of age;

1046 (2) "Consent" has the same meaning as provided in section 42-515, as  
1047 amended by this act;

1048 (3) "Consumer" has the same meaning as provided in section 42-515,  
1049 as amended by this act;

1050 (4) "Controller" has the same meaning as provided in section 42-515,  
1051 as amended by this act;

1052 (5) "Heightened risk of harm to minors" means processing minors'  
1053 personal data in a manner that presents any reasonably foreseeable risk  
1054 of (A) any unfair or deceptive treatment of, or any unlawful disparate  
1055 impact on, minors, (B) any material financial, physical or reputational  
1056 injury to minors, [or] (C) any material physical or other intrusion upon  
1057 the solitude or seclusion, or the private affairs or concerns, of minors if  
1058 such intrusion would be offensive to a reasonable person, (D) any  
1059 physical violence against minors, (E) any material harassment of minors  
1060 on any online service, product or feature, which harassment is severe,  
1061 pervasive or objectively offensive to a reasonable person, or (F) any  
1062 sexual abuse or sexual exploitation of minors;

1063 (6) "HIPAA" has the same meaning as provided in section 42-515, as  
1064 amended by this act;

1065 (7) "Minor" means any consumer who is younger than eighteen years  
1066 of age;

1067 (8) "Online service, product or feature" means any service, product or  
1068 feature that is provided online. "Online service, product or feature" does  
1069 not include any (A) telecommunications service, as defined in 47 USC

1070 153, as amended from time to time, (B) broadband Internet access  
1071 service, as defined in 47 CFR 54.400, as amended from time to time, or  
1072 (C) delivery or use of a physical product;

1073 (9) "Person" has the same meaning as provided in section 42-515, as  
1074 amended by this act;

1075 (10) "Personal data" has the same meaning as provided in section 42-  
1076 515, as amended by this act;

1077 (11) "Precise geolocation data" has the same meaning as provided in  
1078 section 42-515, as amended by this act;

1079 (12) "Process" and "processing" have the same meaning as provided  
1080 in section 42-515, as amended by this act;

1081 (13) "Processor" has the same meaning as provided in section 42-515,  
1082 as amended by this act;

1083 (14) "Profiling" has the same meaning as provided in section 42-515,  
1084 as amended by this act;

1085 (15) "Protected health information" has the same meaning as  
1086 provided in section 42-515, as amended by this act;

1087 (16) "Sale of personal data" has the same meaning as provided in  
1088 section 42-515, as amended by this act;

1089 (17) "Targeted advertising" has the same meaning as provided in  
1090 section 42-515, as amended by this act; and

1091 (18) "Third party" has the same meaning as provided in section 42-  
1092 515, as amended by this act.

1093 Sec. 12. Section 42-529a of the general statutes is repealed and the  
1094 following is substituted in lieu thereof (*Effective February 1, 2026*):

1095 (a) Each controller that offers any online service, product or feature

1096 to consumers whom such controller has actual knowledge, or [wilfully  
1097 disregards] knowledge fairly implied on the basis of objective  
1098 circumstances, are minors shall use reasonable care to avoid any  
1099 heightened risk of harm to minors caused by such online service,  
1100 product or feature. In any enforcement action brought by the Attorney  
1101 General pursuant to section 42-529e, there shall be a rebuttable  
1102 presumption that a controller used reasonable care as required under  
1103 this section if the controller complied with the provisions of section 42-  
1104 529b, as amended by this act, concerning data protection assessments  
1105 and impact assessments.

1106 (b) (1) [Subject to the consent requirement established in subdivision  
1107 (3) of this subsection, no] No controller that offers any online service,  
1108 product or feature to consumers whom such controller has actual  
1109 knowledge, or [wilfully disregards] knowledge fairly implied on the  
1110 basis of objective circumstances, are minors shall [: (A) Process] process  
1111 any minor's personal data; [(i) for] (A) For the purposes of [(I)] (i)  
1112 targeted advertising, [(II)] or (ii) any sale of personal data; [, or (III)]  
1113 profiling in furtherance of any fully automated decision made by such  
1114 controller that produces any legal or similarly significant effect  
1115 concerning the provision or denial by such controller of any financial or  
1116 lending services, housing, insurance, education enrollment or  
1117 opportunity, criminal justice, employment opportunity, health care  
1118 services or access to essential goods or services, (ii)] (B) unless such  
1119 processing is reasonably necessary to provide such online service,  
1120 product or feature; [, (iii)] (C) for any processing purpose [(I)] (i) other  
1121 than the processing purpose that the controller disclosed at the time  
1122 such controller collected such personal data, or [(II)] (ii) that is  
1123 reasonably necessary for, and compatible with, the processing purpose  
1124 described in subparagraph [(A)(iii)(I)] (C)(i) of this subdivision; [, or  
1125 [(iv)] (D) for longer than is reasonably necessary to provide such online  
1126 service, product or feature. [: or (B) use any system design feature to  
1127 significantly increase, sustain or extend any minor's use of such online  
1128 service, product or feature.] The provisions of this subdivision shall not  
1129 apply to any service or application that is used by and under the

1130 direction of an educational entity, including, but not limited to, a  
1131 learning management system or a student engagement program.

1132 (2) [Subject to the consent requirement established in subdivision (3)  
1133 of this subsection, no] No controller that offers an online service,  
1134 product or feature to consumers whom such controller has actual  
1135 knowledge, or [wilfully disregards] knowledge fairly implied on the  
1136 basis of objective circumstances, are minors shall collect a minor's  
1137 precise geolocation data unless: (A) Such precise geolocation data [is  
1138 reasonably] are strictly necessary for the controller to provide such  
1139 online service, product or feature and, if such data [is] are necessary to  
1140 provide such online service, product or feature, such controller may  
1141 only collect such data for the time necessary to provide such online  
1142 service, product or feature; and (B) the controller provides to the minor  
1143 a signal indicating that such controller is collecting such precise  
1144 geolocation data, which signal shall be available to such minor for the  
1145 entire duration of such collection.

1146 (3) (A) Subject to the consent requirement established in  
1147 subparagraph (B) of this subdivision, no controller that offers any online  
1148 service, product or feature to consumers whom such controller has  
1149 actual knowledge, or knowledge fairly implied based on objective  
1150 circumstances, are minors shall process any minor's personal data for  
1151 purposes of profiling in furtherance of any automated decision made by  
1152 such controller that produces any legal or similarly significant effect  
1153 concerning the provision or denial by such controller of any financial or  
1154 lending service, housing, insurance, education enrollment or  
1155 opportunity, criminal justice, employment opportunity, health care  
1156 service or access to any essential good or service, unless such processing  
1157 is reasonably necessary to provide such online service, product or  
1158 feature.

1159 [(3)] (B) No controller shall engage in the activities described in  
1160 [subdivisions (1) and (2) of this subsection] subparagraph (A) of this  
1161 subdivision unless the controller obtains the minor's consent or, if the  
1162 minor is younger than thirteen years of age, the consent of such minor's

1163 parent or legal guardian. A controller that complies with the verifiable  
1164 parental consent requirements established in the Children's Online  
1165 Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations,  
1166 rules, guidance and exemptions adopted pursuant to said act, as said act  
1167 and such regulations, rules, guidance and exemptions may be amended  
1168 from time to time, shall be deemed to have satisfied any requirement to  
1169 obtain parental consent under this [subdivision] subparagraph.

1170 (c) (1) No controller that offers any online service, product or feature  
1171 to consumers whom such controller has actual knowledge, or [wilfully  
1172 disregards] knowledge fairly implied on the basis of objective  
1173 circumstances, are minors shall: (A) Provide any consent mechanism  
1174 that is designed to substantially subvert or impair, or is manipulated  
1175 with the effect of substantially subverting or impairing, user autonomy,  
1176 decision-making or choice; [or] (B) except as provided in subdivision (2)  
1177 of this subsection, offer any direct messaging apparatus for use by  
1178 minors [without providing] unless (i) such controller provides readily  
1179 accessible and easy-to-use safeguards to [limit the ability of adults to  
1180 send] enable any minor, or any minor's parent or legal guardian, to  
1181 prevent any adult from sending any unsolicited [communications to  
1182 minors with whom they are not connected] communication to such  
1183 minor unless such minor and adult are already connected on such online  
1184 service, product or feature, and (ii) the safeguards required under  
1185 subparagraph (B)(i) of this subdivision, as a default setting, prevent any  
1186 adult from sending any unsolicited communication to any minor unless  
1187 such minor and adult are already connected on such online service,  
1188 product or feature; or (C) except as provided in subdivision (3) of this  
1189 subsection, use any system design feature to significantly increase,  
1190 sustain or extend any minor's use of such online service, product or  
1191 feature.

1192 (2) The provisions of subparagraph (B) of subdivision (1) of this  
1193 subsection shall not apply to services where the predominant or  
1194 exclusive function is: (A) Electronic mail; or (B) direct messaging  
1195 consisting of text, photos or videos that are sent between devices by

1196 electronic means, where messages are (i) shared between the sender and  
1197 the recipient, (ii) only visible to the sender and the recipient, and (iii) not  
1198 posted publicly.

1199 (3) The provisions of subparagraph (C) of subdivision (1) of this  
1200 subsection shall not apply to any service or application that is used by  
1201 and under the direction of an educational entity, including, but not  
1202 limited to, a learning management system or a student engagement  
1203 program.

1204 Sec. 13. Section 42-529b of the general statutes is repealed and the  
1205 following is substituted in lieu thereof (*Effective February 1, 2026*):

1206 (a) Each controller that [, on or after October 1, 2024,] offers any online  
1207 service, product or feature to consumers whom such controller has  
1208 actual knowledge, or [wilfully disregards] knowledge fairly implied  
1209 based on objective circumstances, are minors shall conduct a data  
1210 protection assessment for such online service, product or feature: (1) In  
1211 a manner that is consistent with the requirements established in section  
1212 42-522, as amended by this act; and (2) that addresses (A) the purpose  
1213 of such online service, product or feature, (B) the categories of minors'  
1214 personal data that such online service, product or feature processes, (C)  
1215 the purposes for which such controller processes minors' personal data  
1216 with respect to such online service, product or feature, and (D) any  
1217 heightened risk of harm to minors that is a reasonably foreseeable result  
1218 of offering such online service, product or feature to minors.

1219 (b) Each controller that offers any online service, product or feature  
1220 to consumers whom such controller has actual knowledge, or  
1221 knowledge fairly implied based on objective circumstances, are minors  
1222 shall, if such online service, product or feature engages in any profiling  
1223 based on such consumers' personal data, conduct an impact assessment  
1224 for such online service, product or feature. Such impact assessment shall  
1225 include, to the extent reasonably known by or available to the controller,  
1226 as applicable: (1) A statement by the controller disclosing the purpose,  
1227 intended use cases and deployment context of, and benefits afforded by,

1228 such online service, product or feature, if such online service, product  
1229 or feature engages in any profiling for the purpose of making decisions  
1230 that produce legal or similarly significant effects concerning such  
1231 consumers; (2) an analysis of whether such profiling poses any  
1232 reasonably foreseeable heightened risk of harm to minors and, if so, (A)  
1233 the nature of such heightened risk of harm to minors, and (B) the steps  
1234 that have been taken to mitigate such heightened risk of harm to minors;  
1235 (3) a description of (A) the categories of personal data such online  
1236 service, product or feature processes as inputs for the purposes of such  
1237 profiling, and (B) the outputs such online service, product or feature  
1238 produces for the purposes of such profiling; (4) an overview of the  
1239 categories of personal data the controller used to customize such online  
1240 service, product or feature for the purposes of such profiling, if the  
1241 controller used data to customize such online service, product or feature  
1242 for the purposes of such profiling; (5) a description of any transparency  
1243 measures taken concerning such online service, product or feature with  
1244 respect to such profiling, including, but not limited to, any measures  
1245 taken to disclose to consumers that such online service, product or  
1246 feature is being used for such profiling while such online service,  
1247 product or feature is being used for such profiling; and (6) a description  
1248 of the post-deployment monitoring and user safeguards provided  
1249 concerning such online service, product or feature for the purposes of  
1250 such profiling, including, but not limited to, the oversight, use and  
1251 learning processes established by the controller to address issues arising  
1252 from deployment of such online service, product or feature for the  
1253 purposes of such profiling.

1254 [(b)] (c) Each controller that conducts a data protection assessment  
1255 pursuant to subsection (a) of this section, or an impact assessment  
1256 pursuant to subsection (b) of this section, shall: (1) Review such data  
1257 protection assessment or impact assessment as necessary to account for  
1258 any material change to the processing or profiling operations of the  
1259 online service, product or feature that is the subject of such data  
1260 protection assessment or impact assessment; and (2) maintain  
1261 documentation concerning such data protection assessment or impact



1262 assessment for the longer of (A) the three-year period beginning on the  
1263 date on which such processing or profiling operations cease, or (B) as  
1264 long as such controller offers such online service, product or feature.

1265 [(c)] (d) A single data protection assessment or impact assessment  
1266 may address a comparable set of processing or profiling operations that  
1267 include similar activities.

1268 [(d)] (e) If a controller conducts a data protection assessment or  
1269 impact assessment for the purpose of complying with another  
1270 applicable law or regulation, the data protection assessment or impact  
1271 assessment shall be deemed to satisfy the requirements established in  
1272 this section if such data protection assessment or impact assessment is  
1273 reasonably similar in scope and effect to the data protection assessment  
1274 or impact assessment that would otherwise be conducted pursuant to  
1275 this section.

1276 [(e)] (f) If any controller conducts a data protection assessment  
1277 pursuant to subsection (a) of this section, or an impact assessment  
1278 pursuant to subsection (b) of this section, and determines that the online  
1279 service, product or feature that is the subject of such assessment poses a  
1280 heightened risk of harm to minors, such controller shall establish and  
1281 implement a plan to mitigate or eliminate such risk. The Attorney  
1282 General may require a controller to disclose to the Attorney General a  
1283 plan established pursuant to this subsection if the plan is relevant to an  
1284 investigation conducted by the Attorney General. The controller shall  
1285 disclose such plan to the Attorney General not later than ninety days  
1286 after the Attorney General notifies the controller, in a form and manner  
1287 prescribed by the Attorney General, that the Attorney General requires  
1288 the controller to disclose such plan to the Attorney General.

1289 [(f)] (g) Data protection assessments, impact assessments and harm  
1290 mitigation or elimination plans shall be confidential and shall be exempt  
1291 from disclosure under the Freedom of Information Act, as defined in  
1292 section 1-200. To the extent any information contained in a data  
1293 protection assessment, impact assessment or harm mitigation or

1294 elimination plan disclosed to the Attorney General includes information  
1295 subject to the attorney-client privilege or work product protection, such  
1296 disclosure shall not constitute a waiver of such privilege or protection.

1297 Sec. 14. Subsection (a) of section 42-529c of the general statutes is  
1298 repealed and the following is substituted in lieu thereof (*Effective*  
1299 *February 1, 2026*):

1300 (a) A processor shall adhere to the instructions of a controller, and  
1301 shall: (1) Assist the controller in meeting the controller's obligations  
1302 under sections 42-529 to 42-529e, inclusive, as amended by this act,  
1303 taking into account (A) the nature of the processing, (B) the information  
1304 available to the processor by appropriate technical and organizational  
1305 measures, and (C) whether such assistance is reasonably practicable and  
1306 necessary to assist the controller in meeting such obligations; and (2)  
1307 provide any information that is necessary to enable the controller to  
1308 conduct and document data protection assessments and impact  
1309 assessments pursuant to section 42-529b, as amended by this act.

1310 Sec. 15. Subsection (d) of section 42-529d of the general statutes is  
1311 repealed and the following is substituted in lieu thereof (*Effective*  
1312 *February 1, 2026*):

1313 (d) No obligation imposed on a controller or processor under any  
1314 provision of sections 42-529 to 42-529c, inclusive, as amended by this  
1315 act, or section 42-529e shall be construed to restrict a controller's or  
1316 processor's ability to collect, use or retain data for internal use to: (1)  
1317 Conduct internal research to develop, improve or repair products,  
1318 services or technology; (2) effectuate a product recall; (3) identify and  
1319 repair technical errors that impair existing or intended functionality; (4)  
1320 process personal data for the purposes of profiling in furtherance of any  
1321 automated decision that may produce any legal or similarly significant  
1322 effect concerning a consumer, provided such personal data are (A)  
1323 processed only to the extent necessary to detect or correct any bias that  
1324 may result from processing such personal data for such purposes, such  
1325 bias cannot effectively be detected or corrected without processing such

1326 personal data and such personal data are deleted once such processing  
1327 has been completed, (B) processed subject to appropriate safeguards to  
1328 protect the rights of consumers secured by the Constitution or laws of  
1329 this state or of the United States, (C) subject to technical restrictions  
1330 concerning the reuse of such personal data and industry-standard  
1331 security and privacy measures, including, but not limited to,  
1332 pseudonymization, (D) subject to measures to ensure that such personal  
1333 data are secure, protected and subject to suitable safeguards, including,  
1334 but not limited to, strict controls concerning, and documentation of,  
1335 access to such personal data, to avoid misuse and ensure that only  
1336 authorized persons may access such personal data while preserving the  
1337 confidentiality of such personal data, and (E) not transmitted,  
1338 transferred or otherwise accessed by any third party; or [(4)] (5) perform  
1339 solely internal operations that are (A) reasonably aligned with the  
1340 expectations of a minor or reasonably anticipated based on the minor's  
1341 existing relationship with the controller or processor, or (B) otherwise  
1342 compatible with processing data in furtherance of the provision of a  
1343 product or service specifically requested by a minor.

1344       Sec. 16. (NEW) (*Effective October 1, 2025*) (a) As used in this section:

1345       (1) "Brokered personal data" means any personal data that are  
1346 categorized or organized for the purpose of enabling a data broker to  
1347 sell or license such personal data to another person;

1348       (2) "Business" (A) means (i) a person who regularly engages in  
1349 commercial activities for the purpose of generating income, (ii) a bank,  
1350 Connecticut credit union, federal credit union, out-of-state bank, out-of-  
1351 state trust company or out-of-state credit union, as said terms are  
1352 defined in section 36a-2 of the general statutes, and (iii) any other person  
1353 that controls, is controlled by or is under common control with a person  
1354 described in subparagraph (A)(i) or (A)(ii) of this subdivision, and (B)  
1355 does not include any body, authority, board, bureau, commission,  
1356 district or agency of this state or of any political subdivision of this state;

1357       (3) "Consumer" has the same meaning as provided in section 42-515

1358 of the general statutes, as amended by this act;

1359 (4) "Data broker" means any business or, if such business is an entity,  
1360 any portion of such business that sells or licenses brokered personal data  
1361 to another person;

1362 (5) "Department" means the Department of Consumer Protection;

1363 (6) "License" (A) means to grant access to, or distribute, personal data  
1364 in exchange for consideration, and (B) does not include any use of  
1365 personal data for the sole benefit of the person who provided such  
1366 personal data if such person maintains control over the use of such  
1367 personal data;

1368 (7) "Person" has the same meaning as provided in section 42-515 of  
1369 the general statutes, as amended by this act; and

1370 (8) "Personal data" (A) means any data concerning a consumer that,  
1371 either alone or in combination with any other data that are sold or  
1372 licensed by a data broker to another person, can reasonably be  
1373 associated with the consumer, and (B) includes, but is not limited to, (i)  
1374 a consumer's name or the name of any member of the consumer's  
1375 immediate family or household, (ii) a consumer's address or the address  
1376 of any member of the consumer's immediate family or household, (iii) a  
1377 consumer's birth date or place of birth, (iv) the maiden name of a  
1378 consumer's mother, (v) biometric data, as defined in section 42-515 of  
1379 the general statutes, as amended by this act, concerning a consumer, and  
1380 (vi) a consumer's Social Security number or any other government-  
1381 issued identification number issued to the consumer.

1382 (b) (1) Except as provided in subdivision (4) of this subsection and  
1383 subsection (d) of this section, no data broker shall sell or license  
1384 brokered personal data in this state unless the data broker is actively  
1385 registered with the Department of Consumer Protection in accordance  
1386 with the provisions of this subsection. A data broker who desires to sell  
1387 or license brokered personal data in this state shall submit an  
1388 application to the department in a form and manner prescribed by the

1389 Commissioner of Consumer Protection. Each application for  
1390 registration as a data broker shall be accompanied by a registration fee  
1391 in the amount of one thousand two hundred dollars. Each registration  
1392 issued pursuant to this subsection shall expire on December thirty-first  
1393 of the year in which such registration was issued and may be renewed  
1394 for successive one-year terms upon application made in the manner set  
1395 forth in this subsection and payment of a registration renewal fee in the  
1396 amount of one thousand two hundred dollars.

1397 (2) Except as provided in subdivision (4) of this subsection, each  
1398 application submitted to the department pursuant to subdivision (1) of  
1399 this subsection shall include:

1400 (A) The applicant's name, mailing address, electronic mail address  
1401 and telephone number;

1402 (B) The address of the applicant's primary Internet web site; and

1403 (C) A statement by the applicant disclosing the measures the  
1404 applicant shall take to ensure that no personal data are sold or licensed  
1405 in violation of the provisions of sections 42-515 to 42-525, inclusive, of  
1406 the general statutes, as amended by this act.

1407 (3) The department shall make all information that an applicant  
1408 submits to the department pursuant to subdivision (2) of this subsection  
1409 publicly available on the department's Internet web site.

1410 (4) The department may approve and renew an application for  
1411 registration as a data broker in accordance with the terms of an  
1412 agreement between the department and the Nationwide Multistate  
1413 Licensing System.

1414 (c) No data broker shall sell or license any personal data in violation  
1415 of the provisions of sections 42-515 to 42-525, inclusive, of the general  
1416 statutes, as amended by this act. Each data broker shall implement  
1417 measures to ensure that the data broker does not sell or license any  
1418 personal data in violation of the provisions of sections 42-515 to 42-525,

1419 inclusive, of the general statutes, as amended by this act.

1420 (d) (1) The provisions of this section shall not apply to: (A) A  
1421 consumer reporting agency, as defined in 15 USC 1681a(f), as amended  
1422 from time to time, a person that furnishes information to a consumer  
1423 reporting agency, as provided in 15 USC 1681s-2, as amended from time  
1424 to time, or a user of a consumer report, as defined in 15 USC 1681a(d),  
1425 as amended from time to time, to the extent that the consumer reporting  
1426 agency, person or user engages in activities that are subject to regulation  
1427 under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended  
1428 from time to time; (B) a financial institution, an affiliate or a nonaffiliated  
1429 third party, as said terms are defined in 15 USC 6809, as amended from  
1430 time to time, to the extent that the financial institution, affiliate or  
1431 nonaffiliated third party engages in activities that are subject to  
1432 regulation under Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et  
1433 seq., and the regulations adopted thereunder, as said act and regulations  
1434 may be amended from time to time; (C) a business that collects  
1435 information concerning a consumer if the consumer (i) is a customer,  
1436 subscriber or user of goods or services sold or offered by the business,  
1437 (ii) is in a contractual relationship with the business, (iii) is an investor  
1438 in the business, (iv) is a donor to the business, or (v) otherwise maintains  
1439 a relationship with the business that is similar to the relationships  
1440 described in subparagraphs (C)(i) to (C)(iv), inclusive, of this  
1441 subdivision; or (D) a business that performs services for, or acts as an  
1442 agent or on behalf of, a business described in subparagraph (C) of this  
1443 subdivision.

1444 (2) No provision of this section shall be construed to prohibit an  
1445 unregistered data broker from engaging in any sale or licensing of  
1446 brokered personal data if such sale or licensing exclusively involves: (A)  
1447 Publicly available information (i) concerning a consumer's business or  
1448 profession, or (ii) sold or licensed as part of a service that provides alerts  
1449 for health or safety purposes; (B) information that is lawfully available  
1450 from any federal, state or local government record; (C) providing digital  
1451 access to any (i) journal, book, periodical, newspaper, magazine or news

1452 media, or (ii) educational, academic or instructional work; (D)  
1453 developing or maintaining an electronic commerce service or software;  
1454 (E) providing directory assistance or directory information services as,  
1455 or on behalf of, a telecommunications carrier; or (F) a one-time or  
1456 occasional disposition of the assets of a business, or any portion of a  
1457 business, as part of a transfer of control over the assets of the business  
1458 that is not part of the ordinary conduct of such business or portion of  
1459 such business.

1460 (e) The Commissioner of Consumer Protection may adopt  
1461 regulations, in accordance with the provisions of chapter 54 of the  
1462 general statutes, to implement the provisions of this section.

1463 (f) The Commissioner of Consumer Protection, after providing notice  
1464 and conducting a hearing in accordance with the provisions of chapter  
1465 54 of the general statutes, may impose a civil penalty of not more than  
1466 five hundred dollars per day for each violation of subsections (b) to (d),  
1467 inclusive, of this section. The sum of civil penalties imposed on a data  
1468 broker pursuant to this subsection shall not exceed ten thousand dollars  
1469 during any calendar year.

1470 Sec. 17. (NEW) (*Effective January 1, 2026*) (a) As used in this section:

1471 (1) "Abuser" means an individual who (A) is identified by a survivor  
1472 pursuant to subsection (b) of this section, and (B) has committed, or  
1473 allegedly committed, a covered act against the survivor making the  
1474 connected vehicle services request;

1475 (2) "Account holder" means an individual who is (A) a party to a  
1476 contract with a covered provider that involves a connected vehicle  
1477 service, or (B) a subscriber, customer or registered user of a connected  
1478 vehicle service;

1479 (3) "Connected vehicle service" means any capability provided by or  
1480 on behalf of a motor vehicle manufacturer that enables a person to  
1481 remotely obtain data from, or send commands to, a covered vehicle,  
1482 including, but not limited to, any such capability provided by way of a

1483 software application that is designed to be operated on a mobile device;

1484 (4) "Connected vehicle service request" means a request by a survivor  
1485 to terminate or disable an abuser's access to a connected vehicle service;

1486 (5) "Covered act" means conduct that constitutes (A) a crime  
1487 described in Section 40002(a) of the Violence Against Women Act of  
1488 1994, 34 USC 12291(a), as amended from time to time, (B) an act or  
1489 practice described in 22 USC 7102(11) or (12), as amended from time to  
1490 time, or (C) a crime, act or practice that is (i) similar to a crime, act or  
1491 practice described in subparagraph (A) or (B) of this subdivision, and  
1492 (ii) prohibited under federal, state or tribal law;

1493 (6) "Covered connected vehicle services account" means an account  
1494 or other means by which a person enrolls in, or obtains access to, a  
1495 connected vehicle service;

1496 (7) "Covered provider" means a motor vehicle manufacturer, or an  
1497 entity acting on behalf of a motor vehicle manufacturer, that provides a  
1498 connected vehicle service;

1499 (8) "Covered vehicle" means a motor vehicle that is (A) the subject of  
1500 a connected vehicle request, and (B) identified by a survivor pursuant  
1501 to subsection (b) of this section;

1502 (9) "Emergency situation" means a situation that, if allowed to  
1503 continue, poses an imminent risk of death or serious bodily harm;

1504 (10) "In-vehicle interface" means a feature or mechanism installed in  
1505 a motor vehicle that allows an individual within the motor vehicle to  
1506 terminate or disable connected vehicle services;

1507 (11) "Person" means an individual, association, company, limited  
1508 liability company, corporation, partnership, sole proprietorship, trust or  
1509 other legal entity; and

1510 (12) "Survivor" means an individual (A) who is eighteen years of age  
1511 or older, and (B) against whom a covered act has been committed or



1512 allegedly committed.

1513 (b) A survivor may submit a connected vehicle service request to a  
1514 covered provider pursuant to this subsection. Each connected vehicle  
1515 service request submitted pursuant to this subsection shall, at a  
1516 minimum, include (1) the vehicle identification number of the covered  
1517 vehicle, (2) the name of the abuser, and (3) (A) proof that the survivor is  
1518 the sole owner of the covered vehicle, (B) if the survivor is not the sole  
1519 owner of the covered vehicle, proof that the survivor is legally entitled  
1520 to exclusive possession of the covered vehicle, which proof may take the  
1521 form of a court order awarding exclusive possession of the covered  
1522 vehicle to the survivor, or (C) if the abuser owns the covered vehicle, in  
1523 whole or in part, a dissolution of marriage decree, restraining order or  
1524 temporary restraining order (i) naming the abuser, and (ii) (I) granting  
1525 exclusive possession of the covered vehicle to the survivor, or (II)  
1526 restricting the abuser's use of a connected vehicle service against the  
1527 survivor.

1528 (c) (1) Not later than two business days after a survivor submits a  
1529 connected vehicle service request to a covered provider pursuant to  
1530 subsection (b) of this section, the covered provider shall take one or  
1531 more of the following actions requested by the survivor in the connected  
1532 vehicle service request, regardless of whether the abuser identified in  
1533 the connected vehicle service request is an account holder: (A)  
1534 Terminate or disable the covered connected vehicle services account  
1535 associated with such abuser; (B) (i) terminate or disable the covered  
1536 connected vehicle services account associated with the covered vehicle,  
1537 including, but not limited to, by resetting or deleting any data or  
1538 wireless connection with respect to the covered vehicle, and (ii) provide  
1539 instructions to the survivor on how to reestablish a covered connected  
1540 vehicle services account; (C) (i) terminate or disable covered connected  
1541 vehicle services for the covered vehicle, including, but not limited to, by  
1542 resetting or deleting any data or wireless connection with respect to the  
1543 covered vehicle, and (ii) provide instructions to the survivor on how to  
1544 reestablish connected vehicle services; or (D) if the motor vehicle has an

1545 in-vehicle interface, provide information to the survivor concerning (i)  
1546 the availability of the in-vehicle interface, and (ii) how to terminate or  
1547 disable connected vehicle services using the in-vehicle interface.

1548 (2) After the covered provider has taken action pursuant to  
1549 subdivision (1) of this subsection, the covered provider shall deny any  
1550 request made by the abuser to obtain any data that (A) were generated  
1551 by the connected vehicle service after the abuser's access to such  
1552 connected vehicle service was terminated or disabled in response to the  
1553 connected vehicle service request, and (B) are maintained by the covered  
1554 provider.

1555 (3) The covered provider shall not refuse to take action pursuant to  
1556 subdivision (1) of this subsection on the basis that any requirement,  
1557 other than a requirement established in subsection (b) of this section, has  
1558 not been satisfied, including, but not limited to, any requirement that  
1559 provides for (A) payment of any fee, penalty or other charge, (B)  
1560 maintaining or extending the term of the covered connected vehicle  
1561 services account, (C) obtaining approval from any account holder other  
1562 than the survivor, or (D) increasing the rate charged for the connected  
1563 vehicle service.

1564 (4) (A) If the covered provider intends to provide any formal notice  
1565 to the abuser regarding any action set forth in subdivision (1) of this  
1566 subsection, the covered provider shall first notify the survivor of the  
1567 date on which the covered provider intends to provide such notice to  
1568 the abuser.

1569 (B) The covered provider shall take reasonable steps to ensure that  
1570 the covered provider only provides formal notice to the abuser,  
1571 pursuant to subparagraph (A) of this subdivision, (i) at least three days  
1572 after the covered provider notified the survivor pursuant to  
1573 subparagraph (A) of this subdivision, and (ii) after the covered provider  
1574 has terminated or disabled the abuser's access to the connected vehicle  
1575 service.

1576 (5) (A) The covered provider shall not be required to take any action  
1577 pursuant to subdivision (1) of this subsection if the covered provider  
1578 cannot operationally or technically effectuate such action.

1579 (B) If the covered provider cannot operationally or technically  
1580 effectuate any action as set forth in subparagraph (A) of this subdivision,  
1581 the covered provider shall promptly notify the survivor who submitted  
1582 the connected vehicle service request that the covered provider cannot  
1583 operationally or technically effectuate such action, which notice shall, at  
1584 a minimum, disclose whether the covered provider's inability to  
1585 operationally or technically effectuate such action can be remedied and,  
1586 if so, any steps the survivor can take to assist the covered provider in  
1587 remedying such inability.

1588 (d) (1) The covered provider and each officer, director, employee,  
1589 vendor or agent of the covered provider shall treat all information  
1590 submitted by the survivor under subsection (b) of this section as  
1591 confidential, and shall securely dispose of such information not later  
1592 than ninety days after the survivor submitted such information.

1593 (2) The covered provider shall not disclose any information  
1594 submitted by the survivor under subsection (b) of this section to a third  
1595 party unless (A) the covered provider has obtained affirmative consent  
1596 from the survivor to disclose such information to the third party, or (B)  
1597 disclosing such information to the third party is necessary to effectuate  
1598 the connected vehicle service request.

1599 (3) Nothing in subdivision (1) of this subsection shall be construed to  
1600 prohibit the covered provider from maintaining, for longer than the  
1601 period specified in subdivision (1) of this subsection, a record that  
1602 verifies that the survivor fulfilled the conditions of the connected vehicle  
1603 service request as set forth in subsection (b) of this section, provided  
1604 such record is limited to what is reasonably necessary and proportionate  
1605 to verify that the survivor fulfilled such conditions.

1606 (e) The survivor shall take reasonable steps to notify the covered

1607 provider of any change in the ownership or possession of the covered  
 1608 vehicle that materially affects the need for the covered provider to take  
 1609 action pursuant to subdivision (1) of subsection (c) of this section.

1610 (f) The requirements established in this section shall not prohibit or  
 1611 prevent a covered provider from terminating or disabling an abuser's  
 1612 access to a connected vehicle service in an emergency situation after  
 1613 receiving a connected vehicle service request.

1614 (g) Each covered provider shall publicly post, on such covered  
 1615 provider's Internet web site, a statement describing how a survivor may  
 1616 submit a connected vehicle service request to such covered provider.

1617 (h) Each covered provider and each officer, director, employee,  
 1618 vendor or agent of a covered provider shall be immune from any civil  
 1619 liability which might otherwise arise from any act or omission  
 1620 committed by such covered provider, officer, director, employee,  
 1621 vendor or agent pursuant to subsections (a) to (g), inclusive, of this  
 1622 section, provided such act or omission was committed in compliance  
 1623 with the provisions of said subsections."

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

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

Sec. 15	<i>February 1, 2026</i>	42-529d(d)
Sec. 16	<i>October 1, 2025</i>	New section
Sec. 17	<i>January 1, 2026</i>	New section