



General Assembly

Substitute Bill No. 6

February Session, 2022



AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

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

1 Section 1. (NEW) (*Effective July 1, 2023*) As used in this section and
2 sections 2 to 11, inclusive, of this act, unless the context otherwise
3 requires:

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

13 (2) "Authenticate" means to use reasonable means to determine that
14 a request to exercise any of the rights afforded under subdivisions (1) to
15 (4), inclusive, of subsection (a) of section 4 of this act is being made by
16 the consumer who is entitled to exercise such consumer rights with
17 respect to the personal data at issue.

18 (3) "Biometric data" means data generated by automatic
19 measurements of an individual's biological characteristics, such as a
20 fingerprint, a voiceprint, eye retinas, irises or other unique biological
21 patterns or characteristics that are used to identify a specific individual.

22 (4) "Business associate" has the same meaning as provided in HIPAA.

23 (5) "Child" has the same meaning as provided in COPPA.

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

34 (7) "Consumer" means an individual who is a resident of this state.
35 "Consumer" does not include an individual acting in a commercial or
36 employment context or as an employee, owner, director, officer or
37 contractor of a company, partnership, sole proprietorship, nonprofit or
38 government agency whose communications or transactions with the
39 controller occur solely within the context of that individual's role with
40 the company, partnership, sole proprietorship, nonprofit or government
41 agency.

42 (8) "Controller" means an individual who, or legal entity that, alone
43 or jointly with others determines the purpose and means of processing
44 personal data.

45 (9) "COPPA" means the Children's Online Privacy Protection Act of
46 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and
47 exemptions adopted pursuant to said act, as said act and such
48 regulations, rules, guidance and exemptions may be amended from

49 time to time.

50 (10) "Covered entity" has the same meaning as provided in HIPAA.

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

56 (12) "Decisions that produce legal or similarly significant effects
57 concerning the consumer" means decisions made by the controller that
58 result in the provision or denial by the controller of financial or lending
59 services, housing, insurance, education enrollment or opportunity,
60 criminal justice, employment opportunities, health care services or
61 access to essential goods or services.

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

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

74 (15) "Identified or identifiable individual" means an individual who
75 can be readily identified, directly or indirectly.

76 (16) "Institution of higher education" means any individual who, or
77 school, board, association, limited liability company or corporation that,
78 is licensed or accredited to offer one or more programs of higher

79 learning leading to one or more degrees.

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

85 (18) "Personal data" means any information that is linked or
86 reasonably linkable to an identified or identifiable individual. "Personal
87 data" does not include de-identified data or publicly available
88 information.

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

97 (20) "Process" or "processing" means any operation or set of
98 operations performed, whether by manual or automated means, on
99 personal data or on sets of personal data, such as the collection, use,
100 storage, disclosure, analysis, deletion or modification of personal data.

101 (21) "Processor" means an individual who, or legal entity that,
102 processes personal data on behalf of a controller.

103 (22) "Profiling" means any form of automated processing performed
104 on personal data to evaluate, analyze or predict personal aspects related
105 to an identified or identifiable individual's economic situation, health,
106 personal preferences, interests, reliability, behavior, location or
107 movements.

108 (23) "Protected health information" has the same meaning as

109 provided in HIPAA.

110 (24) "Pseudonymous data" means personal data that cannot be
111 attributed to a specific individual without the use of additional
112 information, provided such additional information is kept separately
113 and is subject to appropriate technical and organizational measures to
114 ensure that the personal data is not attributed to an identified or
115 identifiable individual.

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

121 (26) "Sale of personal data" means the exchange of personal data for
122 monetary or other valuable consideration by the controller to a third
123 party. "Sale of personal data" does not include (A) the disclosure of
124 personal data to a processor that processes the personal data on behalf
125 of the controller, (B) the disclosure of personal data to a third party for
126 purposes of providing a product or service requested by the consumer,
127 (C) the disclosure or transfer of personal data to an affiliate of the
128 controller, (D) the disclosure of personal data where the consumer
129 directs the controller to disclose the personal data or intentionally uses
130 the controller to interact with a third party, (E) the disclosure of personal
131 data that the consumer (i) intentionally made available to the general
132 public via a channel of mass media, and (ii) did not restrict to a specific
133 audience, or (F) the disclosure or transfer of personal data to a third
134 party as an asset that is part of a merger, acquisition, bankruptcy or
135 other transaction, or a proposed merger, acquisition, bankruptcy or
136 other transaction, in which the third party assumes control of all or part
137 of the controller's assets.

138 (27) "Sensitive data" means personal data that includes (A) data
139 revealing racial or ethnic origin, religious beliefs, mental or physical
140 health condition or diagnosis, sex life, sexual orientation or citizenship

141 or immigration status, (B) the processing of genetic or biometric data for
142 the purpose of uniquely identifying an individual, (C) personal data
143 collected from a known child, or (D) precise geolocation data.

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

156 (29) "Third party" means an individual or legal entity, such as a public
157 authority, agency or body, other than the consumer, controller or
158 processor or an affiliate of the processor or the controller.

159 Sec. 2. (NEW) (*Effective July 1, 2023*) The provisions of sections 1 to 11,
160 inclusive, of this act apply to persons that conduct business in this state
161 or persons that produce products or services that are targeted to
162 residents of this state and that during the preceding calendar year: (1)
163 Controlled or processed the personal data of not less than seventy-five
164 thousand consumers, excluding personal data controlled or processed
165 solely for the purpose of completing a payment transaction; or (2)
166 controlled or processed the personal data of not less than twenty-five
167 thousand consumers and derived more than twenty-five per cent of
168 their gross revenue from the sale of personal data.

169 Sec. 3. (NEW) (*Effective July 1, 2023*) (a) The provisions of sections 1 to
170 11, inclusive, of this act do not apply to any: (1) Body, authority, board,
171 bureau, commission, district or agency of this state or of any political
172 subdivision of this state; (2) nonprofit organization; (3) institution of

173 higher education; (4) national securities association that is registered
174 under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended
175 from time to time; (5) financial institution or data subject to Title V of
176 the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or (6) hospital, as
177 defined in section 38a-493 of the general statutes, whether nonprofit or
178 for-profit.

179 (b) The following information and data is exempt from the provisions
180 of sections 1 to 11, inclusive, of this act: (1) Protected health information
181 under HIPAA; (2) patient-identifying information for purposes of 42
182 USC 290dd-2; (3) identifiable private information for purposes of the
183 federal policy for the protection of human subjects under 45 CFR 46; (4)
184 identifiable private information that is otherwise information collected
185 as part of human subjects research pursuant to the good clinical practice
186 guidelines issued by the International Council for Harmonization of
187 Technical Requirements for Pharmaceuticals for Human Use; (5) the
188 protection of human subjects under 21 CFR Parts 6, 50 and 56, or
189 personal data used or shared in research, as defined in 45 CFR 164.501,
190 that is conducted in accordance with the standards set forth in this
191 subdivision and subdivisions (3) and (4) of this subsection, or other
192 research conducted in accordance with applicable law; (6) information
193 and documents created for purposes of the Health Care Quality
194 Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work
195 product for purposes of section 19a-127o of the general statutes and the
196 Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as
197 amended from time to time; (8) information derived from any of the
198 health care related information listed in this subsection that is de-
199 identified in accordance with the requirements for de-identification
200 pursuant to HIPAA; (9) information originating from and intermingled
201 to be indistinguishable with, or information treated in the same manner
202 as, information exempt under this subsection that is maintained by a
203 covered entity or business associate, program or qualified service
204 organization, as specified in 42 USC 290dd-2, as amended from time to
205 time; (10) information used for public health activities and purposes as
206 authorized by HIPAA, community health activities and population

207 health activities; (11) the collection, maintenance, disclosure, sale,
208 communication or use of any personal information bearing on a
209 consumer's credit worthiness, credit standing, credit capacity, character,
210 general reputation, personal characteristics or mode of living by a
211 consumer reporting agency, furnisher or user that provides information
212 for use in a consumer report, and by a user of a consumer report, but
213 only to the extent that such activity is regulated by and authorized
214 under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended
215 from time to time; (12) personal data collected, processed, sold or
216 disclosed in compliance with the Driver's Privacy Protection Act of 1994,
217 18 USC 2721 et seq., as amended from time to time; (13) personal data
218 regulated by the Family Educational Rights and Privacy Act, 20 USC
219 1232g et seq., as amended from time to time; (14) personal data collected,
220 processed, sold or disclosed in compliance with the Farm Credit Act, 12
221 USC 2001 et seq., as amended from time to time; (15) data processed or
222 maintained (A) in the course of an individual applying to, employed by
223 or acting as an agent or independent contractor of a controller, processor
224 or third party, to the extent that the data is collected and used within the
225 context of that role, (B) as the emergency contact information of an
226 individual under sections 1 to 11, inclusive, of this act used for
227 emergency contact purposes, or (C) that is necessary to retain to
228 administer benefits for another individual relating to the individual
229 who is the subject of the information under subdivision (1) of this
230 subsection and used for the purposes of administering such benefits;
231 and (16) personal data collected, processed, sold or disclosed in relation
232 to price, route or service, as such terms are used in the Airline
233 Deregulation Act, 49 USC 40101 et seq., as amended from time to time,
234 by an air carrier subject to said act, to the extent sections 1 to 11,
235 inclusive, of this act are preempted by the Airline Deregulation Act, 49
236 USC 41713, as amended from time to time.

237 (c) Controllers and processors that comply with the verifiable
238 parental consent requirements of COPPA shall be deemed compliant
239 with any obligation to obtain parental consent pursuant to sections 1 to
240 11, inclusive, of this act.

241 Sec. 4. (NEW) (*Effective July 1, 2023*) (a) A consumer shall have the
242 right to: (1) Confirm whether or not a controller is processing the
243 consumer's personal data and access such personal data; (2) correct
244 inaccuracies in the consumer's personal data, taking into account the
245 nature of the personal data and the purposes of the processing of the
246 consumer's personal data; (3) delete personal data provided by, or
247 obtained about, the consumer; (4) obtain a copy of the consumer's
248 personal data processed by the controller, in a portable and, to the extent
249 technically feasible, readily usable format that allows the consumer to
250 transmit the data to another controller without hindrance, where the
251 processing is carried out by automated means, provided such controller
252 shall not be required to reveal any trade secret; and (5) opt out of the
253 processing of the personal data for purposes of (A) targeted advertising,
254 (B) the sale of personal data, except as provided in subsection (b) of
255 section 6 of this act, or (C) profiling in furtherance of solely automated
256 decisions that produce legal or similarly significant effects concerning
257 the consumer.

258 (b) A consumer may exercise rights under this section by a secure and
259 reliable means established by the controller and described to the
260 consumer in the controller's privacy notice. A consumer may designate
261 an authorized agent in accordance with section 5 of this act to exercise
262 the rights of such consumer to opt out of the processing of such
263 consumer's personal data for purposes of subdivision (5) of subsection
264 (a) of this section on behalf of the consumer. In the case of processing
265 personal data of a known child, the parent or legal guardian may
266 exercise such consumer rights on the child's behalf. In the case of
267 processing personal data concerning a consumer subject to a
268 guardianship, conservatorship or other protective arrangement, the
269 guardian or the conservator of the consumer may exercise such rights
270 on the consumer's behalf.

271 (c) Except as otherwise provided in sections 1 to 11, inclusive, of this
272 act, a controller shall comply with a request by a consumer to exercise
273 the consumer rights authorized pursuant to said sections as follows:

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

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

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

294 (4) If a controller is unable to authenticate the request using
295 commercially reasonable efforts, the controller shall not be required to
296 comply with a request to initiate an action pursuant to this section and
297 shall provide notice to the consumer that the controller is unable to
298 authenticate the request until the consumer provides additional
299 information reasonably necessary to authenticate the consumer and the
300 consumer's request.

301 (5) A controller that has obtained personal data about a consumer
302 from a source other than the consumer shall be deemed in compliance
303 with a consumer's request to delete such data pursuant to subdivision
304 (3) of subsection (a) of this section by (A) retaining a record of the
305 deletion request and the minimum data necessary for the purpose of

306 ensuring the consumer's personal data remains deleted from the
307 business's records and not using such retained data for any other
308 purpose pursuant to the provisions of sections 1 to 11, inclusive, of this
309 act, or (B) opting the consumer out of the processing of such personal
310 data for any purpose except for those exempted pursuant to the
311 provisions of sections 1 to 11, inclusive, of this act.

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

323 Sec. 5. (NEW) (*Effective July 1, 2023*) A consumer may designate
324 another person to serve as the consumer's authorized agent, and act on
325 such consumer's behalf, to opt out of the processing of such consumer's
326 personal data for one or more of the purposes specified in subdivision
327 (5) of subsection (a) of section 4 of this act. The consumer may designate
328 such authorized agent by way of, among other things, a technology,
329 including, but not limited to, an Internet link or a browser setting,
330 browser extension or global device setting, indicating such consumer's
331 intent to opt out of such processing. A controller shall comply with an
332 opt-out request received from an authorized agent if the controller is
333 able to authenticate, with commercially reasonable effort, the identity of
334 the consumer and the authorized agent's authority to act on such
335 consumer's behalf.

336 Sec. 6. (NEW) (*Effective July 1, 2023*) (a) A controller shall: (1) Limit
337 the collection of personal data to what is adequate, relevant and
338 reasonably necessary in relation to the purposes for which such data is

339 processed, as disclosed to the consumer; (2) except as otherwise
340 provided in sections 1 to 11, inclusive, of this act, not process personal
341 data for purposes that are neither reasonably necessary to, nor
342 compatible with, the disclosed purposes for which such personal data is
343 processed, as disclosed to the consumer, unless the controller obtains
344 the consumer's consent; (3) establish, implement and maintain
345 reasonable administrative, technical and physical data security practices
346 to protect the confidentiality, integrity and accessibility of personal data
347 appropriate to the volume and nature of the personal data at issue; (4)
348 not process sensitive data concerning a consumer without obtaining the
349 consumer's consent, or, in the case of the processing of sensitive data
350 concerning a known child, without processing such data in accordance
351 with COPPA; (5) not process personal data in violation of the laws of
352 this state and federal laws that prohibit unlawful discrimination against
353 consumers; (6) provide an effective mechanism for a consumer to revoke
354 the consumer's consent under this section that is at least as easy as the
355 mechanism by which the consumer provided the consumer's consent
356 and, upon revocation of such consent, cease to process the data as soon
357 as practicable, but not later than fifteen days after the receipt of such
358 request; and (7) not process the personal data of a consumer for
359 purposes of targeted advertising, or sell the consumer's personal data
360 without the consumer's consent, under circumstances where a controller
361 has actual knowledge, or wilfully disregards, that the consumer is at
362 least thirteen years of age but younger than eighteen years of age. A
363 controller shall not discriminate against a consumer for exercising any
364 of the consumer rights contained in sections 1 to 11, inclusive, of this act,
365 including denying goods or services, charging different prices or rates
366 for goods or services or providing a different level of quality of goods
367 or services to the consumer.

368 (b) Nothing in subsection (a) of this section shall be construed to
369 require a controller to provide a product or service that requires the
370 personal data of a consumer which the controller does not collect or
371 maintain, or prohibit a controller from offering a different price, rate,
372 level, quality or selection of goods or services to a consumer, including

373 offering goods or services for no fee, if the offering is in connection with
374 a consumer's voluntary participation in a bona fide loyalty, rewards,
375 premium features, discounts or club card program. If a consumer
376 exercises the consumer's right to opt out pursuant to subdivision (5) of
377 subsection (a) of section 4 of this act, a controller may not sell the
378 consumer's personal data to a third party as part of such program
379 unless: (1) The sale is reasonably necessary to enable the third party to
380 provide a benefit to which the consumer is entitled; (2) the sale of
381 personal data to third parties is clearly disclosed in the terms of the
382 program; and (3) the third party uses the personal data only for
383 purposes of facilitating such a benefit to which the consumer is entitled
384 and does not retain or otherwise use or disclose the personal data for
385 any other purpose.

386 (c) A controller shall provide consumers with a reasonably accessible,
387 clear and meaningful privacy notice that includes: (1) The categories of
388 personal data processed by the controller; (2) the purpose for processing
389 personal data; (3) how consumers may exercise their consumer rights,
390 including how a consumer may appeal a controller's decision with
391 regard to the consumer's request; (4) the categories of personal data that
392 the controller shares with third parties, if any; (5) the categories of third
393 parties, if any, with which the controller shares personal data; and (6)
394 an active electronic mail address that the consumer may use to contact
395 the controller.

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

400 (e) (1) A controller shall establish, and shall describe in a privacy
401 notice, one or more secure and reliable means for consumers to submit
402 a request to exercise their consumer rights pursuant to sections 1 to 11,
403 inclusive, of this act. Such means shall take into account the ways in
404 which consumers normally interact with the controller, the need for
405 secure and reliable communication of such requests and the ability of

406 the controller to authenticate the identity of the consumer making the
407 request. A controller shall not require a consumer to create a new
408 account in order to exercise consumer rights, but may require a
409 consumer to use an existing account. Any such means shall include:

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

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

421 (I) Not unfairly disadvantage another controller;

422 (II) Not make use of a default setting, but, rather, require the
423 consumer to make an affirmative, freely given and unambiguous choice
424 to opt out of any processing of such consumer's personal data pursuant
425 to sections 1 to 11, inclusive, of this act;

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

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

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

434 (B) If a consumer's decision to opt out of any processing of the

435 consumer's personal data for the purposes of targeted advertising, or
436 any sale of such personal data, through an opt-out preference signal sent
437 in accordance with the provisions of subparagraph (A) of this
438 subdivision conflicts with the consumer's existing business-specific
439 privacy setting or participation in a business's financial incentive
440 program, the business shall comply with such consumer's opt-out
441 preference signal but may notify such consumer of such conflict and
442 provide to such consumer the choice to confirm such business-specific
443 privacy setting or participation in such business's financial incentive
444 program.

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

451 Sec. 7. (NEW) (*Effective July 1, 2023*) (a) A processor shall adhere to
452 the instructions of a controller and shall assist the controller in meeting
453 the controller's obligations under sections 1 to 11, inclusive, of this act.
454 Such assistance shall include: (1) Taking into account the nature of
455 processing and the information available to the processor, by
456 appropriate technical and organizational measures, insofar as is
457 reasonably practicable, to fulfill the controller's obligation to respond to
458 consumer rights requests; (2) taking into account the nature of
459 processing and the information available to the processor, by assisting
460 the controller in meeting the controller's obligations in relation to the
461 security of processing the personal data and in relation to the
462 notification of a breach of security, as defined in section 36a-701b of the
463 general statutes, of the system of the processor, in order to meet the
464 controller's obligations; and (3) providing necessary information to
465 enable the controller to conduct and document data protection
466 assessments.

467 (b) A contract between a controller and a processor shall govern the

468 processor's data processing procedures with respect to processing
469 performed on behalf of the controller. The contract shall be binding and
470 clearly set forth instructions for processing data, the nature and purpose
471 of processing, the type of data subject to processing, the duration of
472 processing and the rights and obligations of both parties. The contract
473 shall also require that the processor: (1) Ensure that each person
474 processing personal data is subject to a duty of confidentiality with
475 respect to the data; (2) at the controller's direction, delete or return all
476 personal data to the controller as requested at the end of the provision
477 of services, unless retention of the personal data is required by law; (3)
478 upon the reasonable request of the controller, make available to the
479 controller all information in its possession necessary to demonstrate the
480 processor's compliance with the obligations in sections 1 to 11, inclusive,
481 of this act; (4) engage any subcontractor pursuant to a written contract
482 that requires the subcontractor to meet the obligations of the processor
483 with respect to the personal data; and (5) allow, and cooperate with,
484 reasonable assessments by the controller or the controller's designated
485 assessor, or the processor may arrange for a qualified and independent
486 assessor to conduct an assessment of the processor's policies and
487 technical and organizational measures in support of the obligations
488 under sections 1 to 11, inclusive, of this act, using an appropriate and
489 accepted control standard or framework and assessment procedure for
490 such assessments. The processor shall provide a report of such
491 assessment to the controller upon request.

492 (c) Nothing in this section shall be construed to relieve a controller or
493 processor from the liabilities imposed on the controller or processor by
494 virtue of such controller's or processor's role in the processing
495 relationship, as described in sections 1 to 11, inclusive, of this act.

496 (d) Determining whether a person is acting as a controller or
497 processor with respect to a specific processing of data is a fact-based
498 determination that depends upon the context in which personal data is
499 to be processed. A person who is not limited in such person's processing
500 of personal data pursuant to a controller's instructions, or who fails to

501 adhere to such instructions, is a controller and not a processor with
502 respect to a specific processing of data. A processor that continues to
503 adhere to a controller's instructions with respect to a specific processing
504 of personal data remains a processor. If a processor begins, alone or
505 jointly with others, determining the purposes and means of the
506 processing of personal data, the processor is a controller with respect to
507 such processing.

508 Sec. 8. (NEW) (*Effective July 1, 2023*) (a) A controller shall conduct and
509 document a data protection assessment for each of the controller's
510 processing activities that presents a heightened risk of harm to a
511 consumer. For the purposes of this section, processing that presents a
512 heightened risk of harm to a consumer includes: (1) The processing of
513 personal data for the purposes of targeted advertising; (2) the sale of
514 personal data; (3) the processing of personal data for the purposes of
515 profiling, where such profiling presents a reasonably foreseeable risk of
516 (A) unfair or deceptive treatment of, or unlawful disparate impact on,
517 consumers, (B) financial, physical or reputational injury to consumers,
518 (C) a physical or other intrusion upon the solitude or seclusion, or the
519 private affairs or concerns, of consumers, where such intrusion would
520 be offensive to a reasonable person, or (D) other substantial injury to
521 consumers; and (4) the processing of sensitive data.

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

533 (c) The Attorney General may require that a controller disclose any

534 data protection assessment that is relevant to an investigation
535 conducted by the Attorney General, and the controller shall make the
536 data protection assessment available to the Attorney General. The
537 Attorney General may evaluate the data protection assessment for
538 compliance with the responsibilities set forth in sections 1 to 11,
539 inclusive, of this act. Data protection assessments shall be confidential
540 and shall be exempt from disclosure under the Freedom of Information
541 Act, as defined in section 1-200 of the general statutes. To the extent any
542 information contained in a data protection assessment disclosed to the
543 Attorney General includes information subject to attorney-client
544 privilege or work product protection, such disclosure shall not
545 constitute a waiver of such privilege or protection.

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

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

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

556 Sec. 9. (NEW) (*Effective July 1, 2023*) (a) Any controller in possession
557 of de-identified data shall: (1) Take reasonable measures to ensure that
558 the data cannot be associated with an individual; (2) publicly commit to
559 maintaining and using de-identified data without attempting to re-
560 identify the data; and (3) contractually obligate any recipients of the de-
561 identified data to comply with all provisions of sections 1 to 11,
562 inclusive, of this act.

563 (b) Nothing in sections 1 to 11, inclusive, of this act shall be construed
564 to: (1) Require a controller or processor to re-identify de-identified data

565 or pseudonymous data; or (2) maintain data in identifiable form, or
566 collect, obtain, retain or access any data or technology, in order to be
567 capable of associating an authenticated consumer request with personal
568 data.

569 (c) Nothing in sections 1 to 11, inclusive, of this act shall be construed
570 to require a controller or processor to comply with an authenticated
571 consumer rights request if the controller: (1) Is not reasonably capable
572 of associating the request with the personal data or it would be
573 unreasonably burdensome for the controller to associate the request
574 with the personal data; (2) does not use the personal data to recognize
575 or respond to the specific consumer who is the subject of the personal
576 data, or associate the personal data with other personal data about the
577 same specific consumer; and (3) does not sell the personal data to any
578 third party or otherwise voluntarily disclose the personal data to any
579 third party other than a processor, except as otherwise permitted in this
580 section.

581 (d) The rights afforded under subdivisions (1) to (4), inclusive, of
582 subsection (a) of section 4 of this act shall not apply to pseudonymous
583 data in cases where the controller is able to demonstrate that any
584 information necessary to identify the consumer is kept separately and is
585 subject to effective technical and organizational controls that prevent the
586 controller from accessing such information.

587 (e) A controller that discloses pseudonymous data or de-identified
588 data shall exercise reasonable oversight to monitor compliance with any
589 contractual commitments to which the pseudonymous data or de-
590 identified data is subject and shall take appropriate steps to address any
591 breaches of those contractual commitments.

592 Sec. 10. (NEW) (*Effective July 1, 2023*) (a) Nothing in sections 1 to 11,
593 inclusive, of this act shall be construed to restrict a controller's or
594 processor's ability to: (1) Comply with federal, state or municipal
595 ordinances or regulations; (2) comply with a civil, criminal or regulatory
596 inquiry, investigation, subpoena or summons by federal, state,

597 municipal or other governmental authorities; (3) cooperate with law
598 enforcement agencies concerning conduct or activity that the controller
599 or processor reasonably and in good faith believes may violate federal,
600 state or municipal ordinances or regulations; (4) investigate, establish,
601 exercise, prepare for or defend legal claims; (5) provide a product or
602 service specifically requested by a consumer; (6) perform under a
603 contract to which a consumer is a party, including fulfilling the terms of
604 a written warranty; (7) take steps at the request of a consumer prior to
605 entering into a contract; (8) take immediate steps to protect an interest
606 that is essential for the life or physical safety of the consumer or another
607 individual, and where the processing cannot be manifestly based on
608 another legal basis; (9) prevent, detect, protect against or respond to
609 security incidents, identity theft, fraud, harassment, malicious or
610 deceptive activities or any illegal activity, preserve the integrity or
611 security of systems or investigate, report or prosecute those responsible
612 for any such action; (10) engage in public or peer-reviewed scientific or
613 statistical research in the public interest that adheres to all other
614 applicable ethics and privacy laws and is approved, monitored and
615 governed by an institutional review board that determines, or similar
616 independent oversight entities that determine, (A) whether the deletion
617 of the information is likely to provide substantial benefits that do not
618 exclusively accrue to the controller, (B) the expected benefits of the
619 research outweigh the privacy risks, and (C) whether the controller has
620 implemented reasonable safeguards to mitigate privacy risks associated
621 with research, including any risks associated with re-identification; (11)
622 assist another controller, processor or third party with any of the
623 obligations under sections 1 to 11, inclusive, of this act; or (12) process
624 personal data for reasons of public interest in the area of public health,
625 community health or population health, but solely to the extent that
626 such processing is (A) subject to suitable and specific measures to
627 safeguard the rights of the consumer whose personal data is being
628 processed, and (B) under the responsibility of a professional subject to
629 confidentiality obligations under federal, state or local law.

630 (b) The obligations imposed on controllers or processors under

631 sections 1 to 11, inclusive, of this act shall not restrict a controller's or
632 processor's ability to collect, use or retain data for internal use to: (1)
633 Conduct internal research to develop, improve or repair products,
634 services or technology; (2) effectuate a product recall; (3) identify and
635 repair technical errors that impair existing or intended functionality; or
636 (4) perform internal operations that are reasonably aligned with the
637 expectations of the consumer or reasonably anticipated based on the
638 consumer's existing relationship with the controller, or are otherwise
639 compatible with processing data in furtherance of the provision of a
640 product or service specifically requested by a consumer or the
641 performance of a contract to which the consumer is a party.

642 (c) The obligations imposed on controllers or processors under
643 sections 1 to 11, inclusive, of this act shall not apply where compliance
644 by the controller or processor with said sections would violate an
645 evidentiary privilege under the laws of this state. Nothing in sections 1
646 to 11, inclusive, of this act shall be construed to prevent a controller or
647 processor from providing personal data concerning a consumer to a
648 person covered by an evidentiary privilege under the laws of the state
649 as part of a privileged communication.

650 (d) A controller or processor that discloses personal data to a third-
651 party controller or processor, in compliance with the requirements of
652 sections 1 to 11, inclusive, of this act, is not in violation of said sections
653 if the third-party controller or processor that receives and processes
654 such personal data is in violation of said sections, provided, at the time
655 of disclosing the personal data, the disclosing controller or processor did
656 not have reason to believe that the recipient would violate said sections.
657 A third-party controller or processor receiving personal data from a
658 controller or processor in compliance with the requirements of sections
659 1 to 11, inclusive, of this act is likewise not in violation of said sections
660 for the transgressions of the controller or processor from which such
661 third-party controller or processor receives such personal data.

662 (e) Nothing in sections 1 to 11, inclusive, of this act shall be construed
663 as an obligation imposed on controllers and processors that adversely

664 affects the rights or freedoms of any persons, such as exercising the right
665 to freedom of speech under the First Amendment to the United States
666 Constitution, or applies to the processing of personal data by a person
667 in the course of a purely personal or household activity.

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

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

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

687 Sec. 11. (NEW) (*Effective July 1, 2023*) (a) The Attorney General shall
688 have exclusive authority to enforce violations of sections 1 to 10,
689 inclusive, of this act.

690 (b) During the period beginning on July 1, 2023, and ending on
691 December 31, 2024, the Attorney General shall, prior to initiating any
692 action for a violation of any provision of sections 1 to 10, inclusive, of
693 this act, issue a notice of violation to the controller if the Attorney
694 General determines that a cure is possible. If the controller fails to cure

695 such violation within sixty days of receipt of the notice of violation, the
696 Attorney General may bring an action pursuant to this section. Not later
697 than February 1, 2024, the Attorney General shall submit a report, in
698 accordance with section 11-4a of the general statutes, to the joint
699 standing committee of the General Assembly having cognizance of
700 matters relating to general law disclosing: (1) The number of notices of
701 violation the Attorney General has issued; (2) the nature of each
702 violation; (3) the number of violations that were cured during the sixty-
703 day cure period; and (4) any other matter the Attorney General deems
704 relevant for the purposes of such report.

705 (c) Beginning on January 1, 2025, the Attorney General may, in
706 determining whether to grant a controller or processor the opportunity
707 to cure an alleged violation described in subsection (b) of this section,
708 consider: (1) The number of violations; (2) the size and complexity of the
709 controller or processor; (3) the nature and extent of the controller's or
710 processor's processing activities; (4) the substantial likelihood of injury
711 to the public; and (5) the safety of persons or property.

712 (d) Nothing in sections 1 to 10, inclusive, of this act shall be construed
713 as providing the basis for, or be subject to, a private right of action for
714 violations of said sections or any other law.

715 (e) A violation of the requirements of sections 1 to 10, inclusive, of
716 this act shall constitute an unfair trade practice for purposes of section
717 42-110b of the general statutes and shall be enforced solely by the
718 Attorney General, provided the provisions of section 42-110g of the
719 general statutes shall not apply to such violation.

720 Sec. 12. (*Effective from passage*) (a) Not later than September 1, 2022,
721 the chairpersons of the joint standing committee of the General
722 Assembly having cognizance of matters relating to general law shall
723 convene a working group to:

724 (1) Study how HIPAA-adjacent data is handled and recommend
725 legislation, if any, that is necessary to ensure the protection of HIPAA-

726 adjacent data;

727 (2) Study algorithmic decision-making and make recommendations
728 concerning the proper use of data to reduce bias in such decision-
729 making; and

730 (3) Study other topics concerning data privacy.

731 (b) The chairpersons of the joint standing committee of the General
732 Assembly having cognizance of matters relating to general law shall
733 serve as the chairpersons of the working group, and shall jointly appoint
734 the members of the working group. Such members shall include, but
735 need not be limited to:

736 (1) Representatives from industry, academia, consumer advocacy
737 groups, small and large companies and the office of the Attorney
738 General; and

739 (2) Attorneys with experience in privacy law.

740 (c) The administrative staff of the joint standing committee of the
741 General Assembly having cognizance of matters relating to general law
742 shall serve as administrative staff of the working group.

743 (d) Not later than January 1, 2023, the working group shall submit a
744 report on its findings and recommendations to the joint standing
745 committee of the General Assembly having cognizance of matters
746 relating to general law, in accordance with the provisions of section 11-
747 4a of the general statutes. The working group shall terminate on the date
748 that it submits such report or January 1, 2023, whichever is later.

This act shall take effect as follows and shall amend the following sections:		
Section 1	July 1, 2023	New section
Sec. 2	July 1, 2023	New section
Sec. 3	July 1, 2023	New section
Sec. 4	July 1, 2023	New section

Sec. 5	<i>July 1, 2023</i>	New section
Sec. 6	<i>July 1, 2023</i>	New section
Sec. 7	<i>July 1, 2023</i>	New section
Sec. 8	<i>July 1, 2023</i>	New section
Sec. 9	<i>July 1, 2023</i>	New section
Sec. 10	<i>July 1, 2023</i>	New section
Sec. 11	<i>July 1, 2023</i>	New section
Sec. 12	<i>from passage</i>	New section

Statement of Legislative Commissioners:

In Section 1(12), "a consumer" was changed to "the consumer" for consistency; in Section 1(25), Subpara. designators were inserted, and "information that" was deleted, for clarity; in Section 1(29), "controller," was changed to "controller or", for clarity; in Section 4(a)(1), "data and to" was changed to "data and", for clarity; in Section 4(c)(1), "period, together with" was changed to "period and of", for clarity; in Section 6(a)(7), "of" was deleted, for clarity, and "and" was changed to "or", for consistency; in Section 9(d), "that" was inserted, for clarity; in Section 10(a)(6), "under" was inserted, for clarity; and in Sections 10(a)(10)(A) and 10(a)(10)(C), "if" was changed to "whether", for clarity.

GL *Joint Favorable Subst.*