

HOUSE No.

The Commonwealth of Massachusetts

PRESENTED BY:

Tricia Farley-Bouvier

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act establishing the Massachusetts Consumer Data Privacy Act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>Tricia Farley-Bouvier</i>	<i>2nd Berkshire</i>	<i>1/15/2025</i>
<i>Carmin Lawrence Gentile</i>	<i>13th Middlesex</i>	<i>1/21/2025</i>
<i>James K. Hawkins</i>	<i>2nd Bristol</i>	<i>1/21/2025</i>

HOUSE No.

[Pin Slip]

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Fourth General Court
(2025-2026)**

An Act establishing the Massachusetts Consumer Data Privacy Act.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 An Act establishing the Massachusetts Consumer Data Privacy Act

2 SECTION 1. The General Laws, as appearing in the 2022 Official Edition, are hereby
3 amended by inserting after chapter 93L the following chapter:

4 Chapter 93M. Massachusetts Consumer Data Privacy Act

5 Section 1. Definitions.

6 (a) As used in this chapter, unless the context otherwise requires:

7 (1) “Affiliate” means a legal entity that shares common branding with another legal entity
8 or controls, is controlled by or is under common control with another legal entity. For the
9 purposes of this subdivision, “control” and “controlled” mean:

10 (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares
11 of any class of voting security of a company;

12 (B) control in any manner over the election of a majority of the directors or of individuals
13 exercising similar functions; or

14 (C) the power to exercise controlling influence over the management of a company.

15 (2) “Affirmative Consent” means a clear affirmative act signifying a consumer's freely
16 given, specific, informed and unambiguous authorization for an act or practice after having been
17 informed, in response to a specific request from a controller, provided that:

18 (A) the request is provided to the consumer in a clear and conspicuous stand-alone
19 disclosure;

20 (B) the request includes a description of the processing purpose for which the consumer’s
21 consent is sought and:

22 (1) clearly distinguishes between an act or practice that is necessary to fulfill a request of
23 the consumer and an act or practice that is for another purpose;

24 (2) clearly states the specific categories of personal data that the controller intends to
25 collect, process, or transfer under each act or practice; and

26 (3) is written in easy-to-understand language and includes a prominent heading that
27 would enable a reasonable consumer to identify and understand each act or practice;

28 (C) the request clearly explains the consumer's rights related to consent;

29 (D) the request is made in a manner reasonably accessible to and usable by consumers
30 with disabilities;

31 (E) the request is made prior to the controller’s implementation of the act or practice;

32 (F) the request is made available to the consumer in each language in which the controller
33 provides a product or service for which authorization is sought;

34 (G) the option to refuse to give consent is at least as prominent as the option to give
35 consent and the option to refuse to give consent takes the same number of steps or fewer as the
36 option to give consent; and

37 (H) affirmative consent to an act or practice is not inferred from the inaction of the
38 consumer or the consumer's continued use of a service or product provided by the controller.

39 “Affirmative Consent” does not include:

40 (A) acceptance of a general or broad terms of use or similar document that contains
41 descriptions of personal data processing along with other, unrelated information;

42 (B) hovering over, muting, pausing or closing a given piece of content;

43 (C) agreement obtained through the use of a false, fraudulent, or materially misleading
44 statement or representation; or

45 (D) agreement obtained through the use of dark patterns.

46 (3) “Authenticate” means to use reasonable means to determine that a request to exercise
47 any of the rights afforded under this chapter is being made by, or on behalf of, the consumer who
48 is entitled to exercise such consumer rights with respect to the personal data at issue.

49 (4) “Biometric data” means data generated by automatic measurements of an individual's
50 biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, gait, or other
51 unique biological patterns or characteristics that can be used to identify a specific individual.

52 “Biometric data” does not include:

53 (A) a digital or physical photograph,

54 (B) an audio or video recording, or

55 (C) any data generated from a digital or physical photograph, or an audio or video
56 recording, unless such data is generated to identify a specific individual.

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

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

59 (7) “Collect” means buying, renting, gathering, obtaining, receiving, accessing, or
60 otherwise acquiring personal data by any means.

61 (8) “Consumer” means an individual who is a resident of this state.

62 (9) “Consumer health data” means any personal data that a controller describes or reveals
63 a consumer's past, present, or future physical or mental health condition or diagnosis, and
64 includes, but is not limited to, gender-affirming health data and reproductive or sexual health
65 data;

66 (10) “Contextual advertising” means displaying or presenting an advertisement that does
67 not vary based on the identity of the individual recipient and is based solely on—

68 (A) the immediate content of a webpage or online service within which the advertisement
69 appears; or

70 (B) a specific request of the consumer for information or feedback if displayed in
71 proximity to the results of such request for information;

72 Provided, however, that a controller may use the following types of personal data to
73 display a contextual advertisement so long as the personal data is not used to make inferences
74 about the consumer, profile the consumer, or for any other purpose, and that the consumer may
75 use technical means to obfuscate or change their physical location and to specify a language
76 preference —

77 (A) such technical specifications as are necessary for the ad to be delivered and display
78 properly on a given device;

79 (B) a consumer’s immediate presence in a geographic area with a radius no smaller than
80 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but
81 not including precise geolocation data; or

82 (C) the consumer’s language preferences, as inferred from context, browser settings, or
83 user settings.

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

86 (12) “COPPA” means the Children's Online Privacy Protection Act of 1998, 15 USC
87 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as
88 said act and such regulations, rules, guidance and exemptions may be amended from time to
89 time.

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

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

94 (15) “Decisions that produce legal or similarly significant effects concerning the
95 consumer” means decisions that result in access to, or the provision or denial by the controller of,
96 financial or lending services, housing, insurance, education enrollment or opportunity, criminal
97 justice, employment opportunities, health care services or access to essential goods or services.

98 (16) “De-identified data” means data that does not identify and cannot reasonably be used
99 to infer information about, or otherwise be linked to, an identified or identifiable individual, or a
100 device linked to such individual, if the controller that possesses such data:

101 (A) takes reasonable physical, administrative, and technical measures to ensure that such
102 data cannot be associated with an individual or be used to re-identify any individual or device
103 that identifies or is linked or reasonably linkable to an individual,

104 (B) publicly commits to process such data only in a de-identified fashion and not attempt
105 to re-identify such data, and

106 (C) contractually obligates any recipients of such data to satisfy the criteria set forth in
107 subparagraphs (A) and (B) of this subdivision.

108 (17) “First party” means a consumer-facing controller with which the consumer intends
109 or expects to interact.

110 (18) “First-party advertising” means processing by a first party of its own first-party data
111 for the purposes of advertising and marketing and carried out—

112 (A) through direct communications with a consumer, such as direct mail, email, or text
113 message communications;

114 (B) in a physical location operated by the first party; or

115 (C) through display or presentation of an advertisement on the first party's own website,
116 application or its other online content.

117 "First-party advertising" includes marketing measurement related to such advertising and
118 marketing.

119 (19) "First-party data" means personal data collected directly from a consumer by a first
120 party, including based on a visit by the consumer to or use by the consumer of a website, a
121 physical location, or an online service operated by the first party.

122 (20) "Gender-affirming health care services" means all medical care relating to the
123 treatment of gender dysphoria as set forth in the most recent edition of the American Psychiatric
124 Association's "Diagnostic and Statistical Manual of Mental Disorders" and gender incongruence,
125 as defined in the most recent revision of the "International Statistical Classification of Diseases
126 and Related Health Problems."

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

129 (22) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996,
130 42 USC 1320d et seq., as amended from time to time.

131 (23) "Identified or identifiable individual" means an individual who can be readily
132 identified, directly or indirectly.

133 (24) “Marketing measurement” means measuring and reporting on marketing
134 performance or media performance by the controller, including processing personal data for
135 measurement and reporting of frequency, attribution, and performance.

136 (25) “Minor” means any consumer who is younger than 18 years of age.

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

139 (27) “Personal data” means any information, including derived data and unique
140 identifiers, that is linked or reasonably linkable, alone or in combination with other information,
141 to an identified or identifiable individual or a device that identifies or is linked or reasonably
142 linkable to an individual. “Personal data” does not include de-identified data or publicly
143 available information.

144 (28) “Precise geolocation data” means information derived from technology, including,
145 but not limited to, latitude and longitude coordinates from global positioning system mechanisms
146 or other similar positional data, that reveals the past or present physical location of an individual
147 or device that identifies or is linked or reasonably linkable to 1 or more individuals with
148 precision and accuracy within a radius of one thousand seven hundred fifty feet.

149 “Precise geolocation data” does not include the content of communications, a photograph
150 or video, metadata associated with a photograph or video that cannot be linked to an individual,
151 or any data generated by or connected to advanced utility metering infrastructure systems or
152 equipment for use by a utility.

153 (29) “Process” and “processing” mean any operation or set of operations performed,
154 whether by manual or automated means, on personal data or on sets of personal data, such as the
155 use, storage, disclosure, analysis, deletion or modification of personal data.

156 (30) “Processor” means a person who collects, processes, or transfers personal data on
157 behalf of, and at the direction of, a controller or another processor, or a Federal, State, Tribal, or
158 local government entity.

159 (31) “Profiling” means any form of processing performed on personal data to evaluate,
160 analyze or predict personal aspects including an individual’s economic situation, health, personal
161 preferences, interests, reliability, behavior, location or movements.

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

163 (33) “Publicly available information” means information that has been lawfully made
164 available to the general public from:

165 (A) federal, state or municipal government records, if the person collects, processes, and
166 transfers such information in accordance with any restrictions or terms of use placed on the
167 information by the relevant government entity;

168 (B) widely distributed media; or

169 (C) a disclosure to the general public as required by federal, state, or local law.

170 “Publicly available information” does not include:

171 (A) Any obscene visual depiction, as defined in section 1460 of title 18, United States
172 Code;

173 (B) any inference made exclusively from multiple independent sources of publicly
174 available information that reveals sensitive data with respect to a consumer;

175 (C) biometric data;

176 (D) personal data that is created through the combination of personal data with publicly
177 available information;

178 (E) genetic data, unless otherwise made publicly available by the individual to whom the
179 information pertains;

180 (F) information made available by a consumer on a website or online service made
181 available to all members of the public, for free or for a fee, where the consumer has restricted the
182 information to a specific audience; or

183 (G) intimate images, authentic or computer-generated, known to be nonconsensual.

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

187 (A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment,

188 (B) a social, psychological, behavioral or medical intervention,

189 (C) a surgery or procedure, including, but not limited to, an abortion,

190 (D) a use or purchase of a medication, including, but not limited to, a medication used or
191 purchased for the purposes of an abortion,

192 (E) a bodily function, vital sign or symptom,

193 (F) a measurement of a bodily function, vital sign or symptom, or

194 (G) an abortion, including, but not limited to, medical or nonmedical services, products,
195 diagnostics, counseling or follow-up services for an abortion.

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

198 (36) “Sale of personal data” means the exchange of personal data for monetary or other
199 valuable consideration by the controller to a third party.

200 “Sale of personal data” does not include:

201 (A) the disclosure of personal data to a processor that processes the personal data on
202 behalf of the controller;

203 (B) the disclosure of personal data to a third party for purposes of providing a product or
204 service requested by the consumer;

205 (C) the disclosure or transfer of personal data to an affiliate of the controller;

206 (D) with the consumer’s affirmative consent, the disclosure of personal data where the
207 consumer affirmatively directs the controller to disclose the personal data or intentionally uses
208 the controller to interact with a third party; or

209 (E) the disclosure of personal data that the consumer:

210 (i) intentionally made available to the general public via a channel of mass media; and

211 (ii) did not restrict to a specific audience.

212 (37) “Sensitive data” means personal data that includes:

213 (A) data revealing racial or ethnic origin, color, national origin, religious beliefs, mental
214 or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, status as
215 transgender or non-binary, philosophical beliefs or union membership, status as a military
216 servicemember or veteran, income level or indebtedness, or citizenship or immigration status;

217 (B) consumer health data;

218 (C) genetic or biometric data;

219 (D) personal data of a consumer that a controller knows, or willfully disregards, is a
220 minor;

221 (E) precise geolocation data;

222 (F) a government-issued identifier, including a Social Security number, passport number
223 or driver's license number, that is not required by law to be displayed in public;

224 (G) the online activities of a consumer (or device linked or reasonably linkable to a
225 consumer) over time and across websites, online applications, or mobile applications that do not
226 share common branding, or data generated by profiling performed on such data;

227 (H) account names, passwords, usernames, access codes, security questions or answers,
228 or other credentials and information used to log in to an account or device; or

229 (I) status as a victim of a crime.

230 (38) “Small business” means a controller or processor that meets the following criteria
231 for the period of the 3 preceding calendar years (or for the period during which the controller or
232 processor has been in existence if such period is less than 3 years):

233 (A) The controller or processor’ average annual gross revenues during the period did not
234 exceed \$20,000,000, indexed to the Producer Price Index reported by the Bureau of Labor
235 Statistics;

236 (B) The controller or processor, on average, did not annually collect, process, retain, or
237 transfer the personal data of more than 200,000 individuals during the period for any purpose
238 other than initiating, rendering, billing for, finalizing, completing, or otherwise collecting
239 payment for a requested service or product; and

240 (C) The controller or processor did not transfer personal data to a third party in exchange
241 for revenue, except for purposes of initiating, rendering, billing for, finalizing, completing, or
242 otherwise collecting payment for a requested service or product.

243 (39) “Targeted advertising” means displaying or presenting an online advertisement to a
244 consumer or to a device identified by a unique persistent identifier (or to a group of consumers or
245 devices identified by unique persistent identifiers), if the advertisement is selected based, in
246 whole or in part, on known or predicted preferences, characteristics, behavior, or interests
247 associated with the consumer or a device identified by a unique persistent identifier.

248 “Targeted advertising” includes displaying or presenting an online advertisement for a
249 product or service based on the previous interaction of a consumer or a device identified by a
250 unique persistent identifier with such product or service on a website or online service that does

251 not share common branding with the website or online service displaying or presenting the
252 advertisement, and marketing measurement related to such advertisements.

253 “Targeted advertising” does not include:

254 (A) first-party advertising; or

255 (B) contextual advertising.

256 (40) “Third party” means a person that collects personal data from another person that is
257 not the consumer to whom the data pertains and is not a processor with respect to such data.

258 “Third party” does not include a person that collects personal data from another entity if
259 the two entities are affiliates.

260 (41) “Trade secret” has the same meaning as provided in section 42 of chapter 93.

261 (42) “Transfer” means to disclose, release, disseminate, make available, license, rent, or
262 share personal data to a third party orally, in writing, electronically, or by any other means.

263 (43) "Unique persistent identifier" means a technologically created identifier to the extent
264 that such identifier is reasonably linkable to a consumer or a device that identifies or is linked or
265 reasonably linkable to 1 or more consumers, including device identifiers, Internet Protocol
266 addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer
267 numbers, unique pseudonyms, user aliases, telephone numbers, or other forms of persistent or
268 probabilistic identifiers that are linked or reasonably linkable to 1 or more consumers or devices.

269 The term "unique persistent identifier" does not include an identifier assigned by a
270 controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by

271 a consumer with respect to the collecting, processing, and transfer of personal data or otherwise
272 limiting the collecting, processing, or transfer of personal data.

273 Section 2. Applicability.

274 The provisions of this chapter apply to persons that conduct business in this state or
275 persons that produce products or services that are targeted to residents of this state and that
276 during the preceding calendar year:

277 (a) Collected or processed the personal data of not less than 25,000 consumers, excluding
278 personal data controlled or processed solely for the purpose of completing a payment transaction,
279 so long as all personal data collected or processed for such purpose was deleted or de-identified
280 within 90 days, except when necessary to investigate fraud or as consistent with a business's
281 return policy; or

282 (b) derived revenue from the sale of personal data.

283 Section 3. Scope.

284 (a) The provisions of this chapter do not apply to any Federal, State, Tribal, territorial, or
285 local government entity such as a body, authority, board, bureau, commission, district or agency
286 of the Commonwealth or of any political subdivision of the Commonwealth.

287 (b) The following information and data is exempt from the provisions of this chapter:

288 (1) protected health information that a covered entity or business associate collects or
289 processes in accordance with, or documents that a covered entity or business associate creates for
290 the purpose of complying with HIPAA and regulations promulgated under HIPAA, as in effect
291 on the effective date of this Act;

- 292 (2) patient-identifying information for purposes of 42 USC 290dd-2;
- 293 (3) identifiable private information for purposes of the federal policy for the protection of
294 human subjects under 45 CFR 46;
- 295 (4) identifiable private information that is otherwise information collected as part of
296 human subjects research pursuant to the good clinical practice guidelines issued by the
297 International Council for Harmonization of Technical Requirements for Pharmaceuticals for
298 Human Use;
- 299 (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data
300 used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with
301 the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other
302 research conducted in accordance with applicable law;
- 303 (6) information and documents created for purposes of the Health Care Quality
304 Improvement Act of 1986, 42 USC 11101 et seq.;
- 305 (7) patient safety work product for purposes of the Patient Safety and Quality
306 Improvement Act, 42 USC 299b-21 et seq., as amended from time to time;
- 307 (8) information derived from any of the health care-related information listed in this
308 subsection that is de-identified in accordance with the requirements for de-identification pursuant
309 to HIPAA;
- 310 (9) Personal information collected, processed, or sold subject to Title V of the Gramm-
311 Leach-Bliley Act, 15 USC 6801 et seq.;

312 (10) the collection, maintenance, disclosure, sale, communication or use of any personal
313 information bearing on a consumer's credit worthiness, credit standing, credit capacity, character,
314 general reputation, personal characteristics or mode of living by a consumer reporting agency,
315 furnisher or user that provides information for use in a consumer report, and by a user of a
316 consumer report, but only to the extent that such activity is regulated by and authorized under the
317 Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time;

318 (11) personal data collected, processed, sold or disclosed in compliance with the Driver's
319 Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time;

320 (12) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC
321 1232g et seq., as amended from time to time;

322 (13) personal data collected, processed, sold or disclosed in compliance with the Farm
323 Credit Act, 12 USC 2001 et seq., as amended from time to time;

324 (14) data collected, processed, or maintained

325 (A) in the course of an individual applying to, employed by or acting as an agent or
326 independent contractor of a controller, processor, or third party, to the extent that the data is
327 collected and used within the context of that role,

328 (B) as the emergency contact information of an individual under this chapter used for
329 emergency contact purposes, or;

330 C) that is necessary to retain to administer benefits for another individual relating to the
331 individual who is the subject of the information under subdivision (1) of this subsection and used
332 for the purposes of administering such benefits; and

333 (15) personal data collected, processed, sold or disclosed in relation to price, route or
334 service, as such terms are used in the Federal Aviation Act of 1958, 49 USC 40101 et seq., to the
335 extent this chapter is preempted by the Federal Aviation Act of 1958, and the Airline
336 Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

337 (c) Controllers and processors that comply with the verifiable parental consent
338 requirements of COPPA shall be deemed compliant with any obligation to obtain parental
339 consent pursuant to this chapter.

340 Section 4. Consumer rights.

341 (a) A consumer shall have the right to:

342 (1) Confirm whether or not a controller is collecting or processing the consumer's
343 personal data and access such personal data;

344 (2) obtain from a controller a list of specific third parties, other than natural persons, to
345 which the controller has transferred either (i) the consumer's personal data; or (ii) any personal
346 data;

347 (3) correct inaccuracies in the consumer's personal data, taking into account the nature of
348 the personal data and the purposes of the processing of the consumer's personal data, and instruct
349 a controller or processor to make reasonable efforts to notify all third parties or processors to
350 which the controller has transferred such personal data of such corrections;

351 (4) delete personal data provided by, or obtained about, the consumer, including personal
352 data the consumer provided to the controller, personal data the controller obtained from another
353 source, and derived data and instruct a controller or processor to make reasonable efforts to

354 notify all third parties or processors to which the controller has transferred such personal data of
355 such deletion request;

356 (5) obtain a copy of the consumer's personal data collected or processed by the controller,
357 in a portable and, to the extent technically feasible, readily usable format that allows the
358 consumer to transmit the data to another controller without hindrance, where the processing is
359 carried out by automated means; and

360 (6) opt out of the collection and processing of the personal data for purposes of

361 (A) targeted advertising;

362 (B) the transfer of personal data; or

363 (C) profiling in furtherance of solely automated decisions that produce legal or similarly
364 significant effects concerning the consumer.

365 (b) A consumer may exercise rights under this section by a secure and reliable means
366 established by the controller and described to the consumer in the controller's privacy notice. A
367 consumer may designate an authorized agent in accordance with section 5 of this act to exercise
368 the rights of such consumer specified in this section on behalf of the consumer. In the case of
369 personal data of a known child, the parent or legal guardian may exercise such consumer rights
370 on the child's behalf. In the case of personal data concerning a consumer subject to a
371 guardianship, conservatorship or other protective arrangement, the guardian or the conservator of
372 the consumer may exercise such rights on the consumer's behalf.

373 (c) Except as otherwise provided in this chapter, a controller shall comply with a request
374 by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

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

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

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

390 (4) If a controller is unable to authenticate a request to exercise any of the rights afforded
391 under subdivisions (1) to (5), inclusive, of subsection (a) of this section using commercially
392 reasonable efforts, the controller shall not be required to comply with a request to initiate an
393 action pursuant to this section and shall provide notice to the consumer that the controller is
394 unable to authenticate the request to exercise such right or rights until such consumer provides
395 additional information reasonably necessary to authenticate such consumer and such consumer's
396 request to exercise such right or rights, provided that any such information may not be used for

397 any purposes other than the authentication of such consumer. A controller shall not require
398 authentication to exercise an opt-out request, but a controller may deny an opt-out request if the
399 controller has a good faith, reasonable and documented belief that such request is fraudulent. If a
400 controller denies an opt-out request because the controller believes such request is fraudulent, the
401 controller shall send a notice to the person who made such request disclosing that such controller
402 believes such request is fraudulent, why such controller believes such request is fraudulent and
403 that such controller shall not comply with such request.

404 (5) A controller that has obtained personal data about a consumer from a source other
405 than the consumer shall be deemed in compliance with a consumer's request to delete such data
406 pursuant to subdivision (4) of subsection (a) of this section by deleting the consumer's personal
407 data retained by the controller and retaining a record of the deletion request and the minimum
408 data necessary for the purpose of ensuring the consumer's personal data remains deleted from the
409 controller's records and not using such retained data for any other purpose pursuant to this
410 chapter.

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

420 (e) A controller may not condition, effectively condition, attempt to condition, or attempt
421 to effectively condition the exercise of a right described in this section through—

422 (1) the use of any false, fictitious, fraudulent, or materially misleading statement or
423 representation; or

424 (2) the use of dark patterns.

425 (f) A controller or processor may not collect, process, or transfer personal data in a
426 manner that discriminates against an individual or class of individuals, or otherwise makes
427 unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of
428 individuals' actual or perceived race, color, sex, sexual orientation, gender identity, disability,
429 religion, genetic information, pregnancy or condition related to pregnancy, status as a veteran,
430 ancestry or national origin, or any other basis protected by chapter 151B.

431 (g) Subsection (f) does not apply to:

432 (1) The collection, processing, or transfer of personal data for the sole purpose of:

433 (A) A controller or processor's self-testing to prevent or mitigate unlawful discrimination
434 or otherwise to ensure compliance with state or federal law; or

435 (B) Diversifying an applicant, participant or customer pool; or

436 (2) A private establishment, as described in 42 United States Code, Section 2000a(e).

437 Section 5. Authorized agent.

438 A consumer may designate another person to serve as the consumer's authorized agent,
439 and act on such consumer's behalf, to exercise rights specified in subsection (a) of section 4 of

440 this act. A controller shall comply with a request received from an authorized agent if the
441 controller is able to verify, with commercially reasonable effort, the identity of the consumer and
442 the authorized agent's authority to act on such consumer's behalf.

443 Section 6. Actions of controllers.

444 (a) A controller shall:

445 (1) Limit the collection, processing, and transfer of personal data to what is reasonably
446 necessary to provide or maintain:

447 (A) a specific product or service requested by the consumer to whom the data pertains
448 including any routine administrative, operational, or account-servicing activity, such as billing,
449 shipping, delivery, storage, or accounting; or

450 (B) a communication, that is not an advertisement, by the controller to the consumer
451 reasonably anticipated within the context of the relationship between the controller and the
452 consumer.

453 Except with respect to sensitive data, a controller may process or transfer personal data
454 collected under this subsection to provide first-party advertising or targeted advertising;
455 provided, however, that this paragraph does not permit the processing or transfer of personal data
456 for targeted advertising to a consumer who has opted out of such advertising pursuant to section
457 4, 5, or 6, or to a consumer under circumstances where the controller has knowledge, or willfully
458 disregards, that the consumer is a minor;

459 (2) not collect, process, or transfer sensitive data concerning a consumer except when
460 such collection, processing, or transfer is strictly necessary to provide or maintain a specific
461 product or service requested by the consumer to whom the sensitive data pertains;

462 (3) not sell sensitive data;

463 (4) establish, implement and maintain reasonable administrative, technical and physical
464 data security practices to protect the confidentiality, integrity and accessibility of personal data
465 appropriate to the volume and nature of the personal data at issue, including disposing of
466 personal data in accordance with a retention schedule that requires the deletion of personal data
467 when the data is required to be deleted by law or is no longer necessary for the purpose for which
468 the data was collected, processed, or transferred;

469 (5) not transfer sensitive data concerning a consumer without obtaining the consumer's
470 affirmative consent, or, in the case of the collection or processing of personal data concerning a
471 known child, without collecting or processing such data in accordance with COPPA;

472 (6) provide an effective mechanism for a consumer to revoke the consumer's affirmative
473 consent under this chapter that is at least as easy as the mechanism by which the consumer
474 provided the consumer's affirmative consent and, upon revocation of such affirmative consent,
475 cease to process the data as soon as practicable, but not later than fifteen days after the receipt of
476 such request;

477 (7) not process the personal data of a consumer for purposes of targeted advertising, or
478 sell the consumer's personal data, under circumstances where a controller has actual knowledge,
479 or willfully disregards, that the consumer is a minor; and

480 (8) not discriminate or retaliate against a consumer for exercising any of the consumer
481 rights contained in this chapter, or for refusing to agree to the collection or processing of
482 personal data for a separate product or service, including denying goods or services, charging
483 different prices or rates for goods or services or providing a different level of quality of goods or
484 services to the consumer.

485 (b) Nothing in paragraph (8) of subsection (a) shall be construed to require a controller to
486 provide a product or service that requires the personal data of a consumer which the controller
487 does not collect or maintain, or prohibit a controller from offering a different price, rate, level,
488 quality or selection of goods or services to a consumer, including offering goods or services for
489 no fee, if the offering is in connection with a consumer's voluntary participation in a financial
490 incentive program such as a bona fide loyalty, rewards, premium features, discounts or club card
491 program, provided that the controller may not transfer personal data to a third party as part of
492 such program unless:

493 (1) The transfer is functionally necessary to enable the third party to provide a benefit to
494 which the consumer is entitled;

495 (2) the transfer of personal data to the third party is clearly disclosed in the terms of the
496 program; and

497 (3) the third party uses the personal data only for purposes of facilitating a benefit to
498 which the consumer is entitled and does not process or transfer the personal data for any other
499 purpose.

500 The sale of personal data shall not be considered functionally necessary to provide a
501 financial incentive program. A controller shall not use financial incentive practices that are
502 unjust, unreasonable, coercive or usurious in nature.

503 (c) A controller shall provide consumers with a reasonably accessible, clear and
504 meaningful privacy notice that includes:

505 (1) The categories of personal data collected and processed by the controller, including a
506 separate list of categories of sensitive data collected and processed by the controller, described in
507 a level of detail that provides consumers a meaningful understanding of the type of personal data
508 collected or processed;

509 (2) the purpose for collecting and processing each category of personal data the controller
510 collects or processes described in a way that gives consumers a meaningful understanding of
511 how each category of their personal data will be use;

512 (3) how consumers may exercise their consumer rights, including how a consumer may
513 appeal a controller's decision with regard to the consumer's request;

514 (4) the categories of personal data that the controller transfers to third parties, if any, and
515 the purposes for those transfers;

516 (5) the categories of third parties, if any, to which the controller transfers personal data;

517 (6) The length of time the controller intends to retain each category of personal data, or, if
518 it is not possible to identify the length of time, the criteria used to determine the length of time
519 the controller intends to retain categories of personal data; and

520 (7) an active electronic mail address or other online mechanism that the consumer may
521 use to contact the controller.

522 The privacy notice shall be provided directly to consumers and made available online to
523 the general public. If a controller makes a material change to its privacy notice, the controller
524 shall notify each consumer affected by the material change before implementing the material
525 change with respect to prospectively collected personal data and provide a reasonable
526 opportunity for each consumer to withdraw consent. A controller should provide a reasonable
527 opportunity for each consumer to affirmatively consent to further materially different processing
528 or transfer of previously collected personal data under the changed policy. The controller shall
529 take all reasonable electronic measures to provide direct notification regarding material changes
530 to the privacy notice to each affected consumer, taking into account available technology and the
531 nature of the relationship.

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

536 (e) A controller shall establish, and shall describe in a privacy notice, one or more secure
537 and reliable means for consumers to submit a request to exercise their consumer rights pursuant
538 to this chapter. Such means shall take into account the ways in which consumers normally
539 interact with the controller, the need for secure and reliable communication of such requests and
540 the ability of the controller to verify the identity of the consumer making the request. A

541 controller shall not require a consumer to create a new account in order to exercise consumer
542 rights, but may require a consumer to use an existing account. Any such means shall include:

543 (1) Providing a clear and conspicuous link on the controller's Internet web site to an
544 Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted
545 advertising, the sale of the consumer's personal data, and profiling in furtherance of solely
546 automated decisions that produce legal or similarly significant effects concerning the consumer;
547 and

548 (2) Not later than 18 months after the effective date of this chapter, allowing a consumer
549 to opt out of any collection or processing of the consumer's personal data for the purposes of
550 targeted advertising, or any sale of the consumer's personal data, through an opt-out preference
551 signal sent, with such consumer's consent, by a platform, technology or mechanism to the
552 controller indicating such consumer's intent to opt out of any such processing or sale. Such
553 platform, technology or mechanism shall:

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

555 (ii) Enable the controller to reasonably determine whether the consumer is a resident of
556 this state and whether the consumer has made a legitimate request to opt out of any sale of such
557 consumer's personal data or targeted advertising. For purposes of this subsection, the use of an
558 internet protocol address to estimate the consumer's location shall be considered sufficient to
559 reasonably determine residency.

560 If a consumer's decision to opt out of any processing of the consumer's personal data for
561 the purposes of targeted advertising, or any sale of personal data, through an opt-out preference
562 signal sent in accordance with the provisions of this subsection conflicts with the consumer's

563 existing controller-specific privacy setting or voluntary participation in a controller's financial
564 incentive program, the controller shall comply with such consumer's opt-out preference signal
565 but may notify such consumer of such conflict and provide to such consumer the choice to
566 confirm such controller-specific privacy setting or participation in such program.

567 (f) If a controller responds to consumer opt-out requests received pursuant to subsection
568 (e) of this section by informing the consumer of a change in the price, rate, level, quality, or
569 selection of goods or services, the controller shall present the terms of any financial incentive
570 offered pursuant to subsection (b) of this section for the retention, processing, sale or transfer of
571 the consumer's personal data.

572 Section 7. Responsibilities of processors and controllers.

573 (a) A processor shall adhere to the instructions of a controller and shall assist the
574 controller in meeting the controller's obligations under this chapter. Such assistance shall
575 include:

576 (1) Taking into account the nature of processing and the information available to the
577 processor, by appropriate technical and organizational measures, insofar as is reasonably
578 practicable, to fulfill the controller's obligation to respond to consumer rights requests;

579 (2) taking into account the nature of processing and the information available to the
580 processor, by assisting the controller in meeting the controller's obligations in relation to the
581 security of processing the personal data and in relation to the notification of a breach of security
582 of the system of the processor, in order to meet the controller's obligations; and

583 (3) providing necessary information to enable the controller to conduct and document
584 data protection assessments.

585 (b) A contract between a controller and a processor shall govern the processor's data
586 processing procedures with respect to processing performed on behalf of the controller. The
587 contract shall be written, binding and clearly set forth instructions for processing data, the nature
588 and purpose of processing, the type of data subject to processing, the duration of processing and
589 the rights and obligations of both parties including a method by which the processor shall notify
590 the covered entity of material changes to its privacy practices. The processor shall adhere to the
591 instructions of the controller and only process and transfer the data it receives from the controller
592 to the extent necessary to provide a service requested by the controller, as set out in the contract.
593 The contract shall also require that the processor:

594 (1) Ensure that each person processing personal data is subject to a duty of confidentiality
595 with respect to the data;

596 (2) at the controller's direction, delete or return all personal data to the controller as
597 requested at the end of the provision of services, unless retention of the personal data is required
598 by law;

599 (3) upon the reasonable request of the controller, make available to the controller all
600 information in its possession necessary to demonstrate the processor's compliance with the
601 obligations in this chapter;

602 (4) after providing the controller an opportunity to object, engage any subcontractor
603 pursuant to a written contract that requires the subcontractor to meet the contractual and statutory
604 or regulatory obligations of the processor with respect to the personal data;

605 (5) be prohibited from combining personal data that the processor receives from or on
606 behalf of a controller with personal data that the processor receives from or on behalf of another
607 person or collects from the interaction of the processor with an individual; and

608 (6) allow, and cooperate with, reasonable assessments by the controller or the controller's
609 designated assessor, or the processor may arrange for a qualified and independent assessor to
610 conduct an assessment of the processor's policies and technical and organizational measures in
611 support of the obligations under this chapter, using an appropriate and accepted control standard
612 or framework and assessment procedure for such assessments. The processor shall provide a
613 report of such assessment to the controller upon request.

614 (c) A processor shall establish, implement and maintain reasonable administrative,
615 technical and physical data security practices to protect the confidentiality, integrity and
616 accessibility of personal data that are consistent with chapter 93H and appropriate to the volume
617 and nature of the personal data at issue.

618 (d) Nothing in the contract in subsection (b) shall relieve a controller or processor from
619 the liabilities imposed on the controller or processor by virtue of such controller's or processor's
620 role in the processing relationship, as described in this chapter.

621 (e) Determining whether a person is acting as a controller or processor with respect to a
622 specific processing of data is a fact-based determination that depends upon the context in which
623 personal data is to be processed. A person who is not limited in such person's processing of
624 personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is
625 a controller and not a processor with respect to a specific processing of data. A processor that
626 continues to adhere to a controller's instructions with respect to a specific processing of personal

627 data remains a processor. If a processor begins, alone or jointly with others, determining the
628 purposes and means of the processing of personal data, the processor is a controller with respect
629 to such processing and may be subject to an enforcement action under this chapter.

630 (f) A processor shall not process or transfer personal data on the behalf of a controller if
631 the processor has actual knowledge that the controller has violated this chapter with respect to
632 such personal data.

633 Section 8. Data Protection Assessments.

634 (a) A controller shall not conduct processing that presents a heightened risk of harm to a
635 consumer without conducting and documenting a data protection assessment for each of the
636 controller's processing activities that presents such heightened risk of harm to a consumer. For
637 the purposes of this section, processing that presents a heightened risk of harm to a consumer
638 includes:

639 (1) The collection or processing of personal data for the purposes of targeted advertising;

640 (2) the sale of personal data;

641 (3) the processing of personal data for the purposes of profiling, where such profiling
642 presents a reasonably foreseeable risk of:

643 (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

644 (B) financial, physical or reputational injury to consumers,

645 (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or
646 concerns, of consumers, where such intrusion would be offensive to a reasonable person, or

647 (D) other substantial injury to consumers; and

648 (4) the collection or processing of sensitive data.

649 (b) Data protection assessments conducted pursuant to subsection (a) of this section shall
650 identify the categories of personal data collected, the purposes for collecting such personal data,
651 whether personal data is being transferred, and identify and weigh the benefits that may flow,
652 directly and indirectly, from the processing to the controller, the consumer, other stakeholders
653 and the public against the potential risks to the rights of the consumer associated with such
654 processing, as mitigated by safeguards that are employed by the controller to reduce such risks.
655 The controller shall factor into any such data protection assessment the use of de-identified data
656 and the reasonable expectations of consumers, as well as the context of the processing and the
657 relationship between the controller and the consumer whose personal data will be processed.

658 (c) No later than 30 days after completing a data protection assessment under this section,
659 a controller shall submit a report of the data protection assessment or evaluation to the Attorney
660 General. The report must include a summary of the data protection assessment and the controller
661 shall make the summary publicly available in a place that is easily accessible to consumers.
662 Controllers may redact trade secrets or other confidential or proprietary information from the
663 report. The Attorney General may require that a controller disclose any data protection
664 assessment that is relevant to an investigation conducted by the Attorney General, and the
665 controller shall make the data protection assessment available to the Attorney General. The
666 Attorney General may evaluate the data protection assessment for compliance with the
667 responsibilities set forth in this chapter. To the extent any information contained in a data
668 protection assessment disclosed to the Attorney General includes information subject to attorney-

669 client privilege or work product protection, such disclosure shall not constitute a waiver of such
670 privilege or protection.

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

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

678 (f) A controller shall conduct and document a data protection assessment before initiating
679 a processing activity that presents a heightened risk of harm to a consumer and shall review and
680 update the data protection assessment as often as appropriate considering the type, amount, and
681 sensitivity of personal data collected or processed and level of risk presented by the processing,
682 throughout the processing activity's lifecycle in order to:

683 (1) monitor for harm caused by the processing and adjust safeguards accordingly; and

684 (2) ensure that data protection and privacy are considered as the controller makes new
685 decisions with respect to the processing.

686 Section 9. De-identified data.

687 (a) Any controller in possession of de-identified data shall:

688 (1) Take technical measures to ensure that the data cannot be associated with an
689 individual;

690 (2) publicly commit to maintaining and using de-identified data without attempting to re-
691 identify the data; and

692 (3) contractually obligate any recipients of the de-identified data to comply with all
693 provisions of this chapter.

694 (b) Nothing in this chapter shall be construed to:

695 (1) Require a controller or processor to re-identify de-identified data; or

696 (2) maintain data in identifiable form, or collect, obtain, retain or access any data or
697 technology, in order to be capable of associating an authenticated consumer request with
698 personal data.

699 (c) Nothing in this chapter shall be construed to require a controller or processor to
700 comply with an authenticated consumer rights request if the controller:

701 (1) Is not reasonably capable of associating the request with the personal data or it would
702 be unreasonably burdensome for the controller to associate the request with the personal data;
703 and

704 (2) does not use the personal data to recognize or respond to the specific consumer who is
705 the subject of the personal data, or associate the personal data with other personal data about the
706 same specific consumer;

707 (d) A controller that transfers de-identified data shall exercise reasonable oversight to
708 monitor compliance with any contractual commitments to which the de-identified data is subject
709 and shall take appropriate steps to address any breaches of those contractual commitments.

710 Section 10. Limitations.

711 (a) Nothing in this chapter shall be construed to restrict a controller's or processor's
712 ability to:

713 (1) Comply with federal, state or municipal ordinances or regulations;

714 (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or
715 summons by federal, state, municipal or other governmental authorities;

716 (3) cooperate with law enforcement agencies concerning conduct or activity that the
717 controller or processor reasonably and in good faith believes may violate federal, state or
718 municipal ordinances or regulations;

719 (4) investigate, establish, exercise, prepare for or defend legal claims;

720 (5) provide a product or service specifically requested by the consumer;

721 (6) perform under a contract to which a consumer is a party, including fulfilling the terms
722 of a written warranty;

723 (7) take steps at the request of a consumer prior to entering into a contract;

724 (8) take immediate steps to protect an interest that is essential for the life or physical
725 safety of the consumer or another individual, and where the processing cannot be manifestly
726 based on another legal basis;

727 (9) prevent, detect, protect against or respond to security incidents, identity theft, fraud,
728 harassment, malicious or deceptive activities or any illegal activity targeted at or involving the
729 controller or processor or its services, preserve the integrity or security of systems or investigate,

730 report or prosecute those responsible for any such action, provided that for the purposes of this
731 paragraph, “illegal activity” means a violation of a federal, state, or local law punishable as a
732 felony or misdemeanor that can directly harm;

733 (10) engage in public or peer-reviewed scientific, historical, or statistical research in the
734 public interest that adheres to all relevant laws and regulations governing such research, if
735 applicable, and is approved, monitored and governed by an institutional review board that
736 determines, or similar independent oversight entities that determine,

737 (A) whether the deletion of personal data requested by a consumer under section 4,
738 subsection (a), subparagraph (4) is likely to provide substantial benefits that do not exclusively
739 accrue to the controller,

740 (B) the expected benefits of the research outweigh the privacy risks, and

741 (C) whether the controller has implemented reasonable safeguards to mitigate privacy
742 risks associated with research, including any risks associated with re-identification;

743 (11) assist another controller, processor or third party with any of the obligations under
744 this chapter;

745 (12) process personal data for reasons of public interest in the area of public health,
746 community health or population health, but solely to the extent that such processing is

747 (A) subject to suitable and specific measures to safeguard the rights of the consumer
748 whose personal data is being processed, and

749 (B) under the responsibility of a professional subject to confidentiality obligations under
750 federal, state or local law;

751 (13) ensure the data security and integrity of personal data as required by this chapter,
752 protect against spam, or protect and maintain networks and systems, including through
753 diagnostics, debugging, and repairs;

754 (14) transfer assets to a third party in the context of a merger, acquisition, bankruptcy or
755 similar transaction when the third party assumes control, in whole or in part, of the controller's
756 assets, only if the controller, in a reasonable time prior to the transfer, provides an affected
757 consumer with:

758 (A) A notice describing the transfer, including the name of the entity receiving the
759 consumer's personal data and the applicable privacy policies of such entity and

760 (B) a reasonable opportunity to:

761 (i) withdraw previously provided consent related to the consumer's personal data, and

762 (ii) request the deletion of the consumer's personal data;

763 (15) effectuate a product recall pursuant to federal or state law, or to fulfill a warranty;

764 (16) conduct medical research in compliance with part 46 of title 45, Code of Federal
765 Regulations, or parts 50 and 56 of title 21, Code of Federal Regulations

766 (17) publish entity-based member or employee contact information where such
767 publication is intended to allow members of the public to contact such member or employee in
768 the ordinary course of the entity's operations; or

769 (18) process personal data previously collected in accordance with this chapter such that
770 the personal data becomes de-identified data, including to:

771 (A) Conduct internal research to develop, improve or repair products, services or
772 technology;

773 (B) identify and repair technical errors that impair existing or intended functionality; or;

774 (C) perform internal operations that are reasonably aligned with the expectations of the
775 consumer or reasonably anticipated based on the consumer's existing relationship with the
776 controller, or are otherwise compatible with processing data in furtherance of the provision of a
777 product or service specifically requested by a consumer or the performance of a contract to
778 which the consumer is a party.

779 (b) The obligations imposed on controllers or processors under this chapter shall not
780 apply where compliance by the controller or processor with said sections would violate an
781 evidentiary privilege under the laws of this state. Nothing in this chapter shall be construed to
782 prevent a controller or processor from providing personal data concerning a consumer to a
783 person covered by an evidentiary privilege under the laws of the state as part of a privileged
784 communication.

785 (c) A controller or processor that discloses personal data to a processor or third-party
786 controller in accordance with this chapter shall not be deemed to have violated said sections if
787 the processor or third-party controller that receives and processes such personal data violates said
788 sections, provided, at the time the disclosing controller or processor disclosed such personal data,
789 the disclosing controller or processor did not have actual knowledge that the receiving processor
790 or third-party controller would violate said sections. A third-party controller or processor
791 receiving personal data from a controller or processor in compliance with this chapter is likewise

792 not in violation of said sections for the transgressions of the controller or processor from which
793 such third-party controller or processor receives such personal data.

794 (d) Nothing in this chapter shall be construed to:

795 (1) Impose any obligation on a controller or processor that adversely affects the rights or
796 freedoms of any person, including, but not limited to, the rights of any person to freedom of
797 speech or freedom of the press guaranteed in the First Amendment to the United States
798 Constitution or Article 16 of the Massachusetts Declaration of Rights;

799 (2) apply to any person's collection or processing of personal data in the course of such
800 person's purely personal or household activities; or

801 (3) for private schools approved under section 1 of chapter 76 and private institutions of
802 higher education as defined by title I of the Higher Education Act of 1965, 20 United States
803 Code, Section 1001 et seq., require deletion of personal data that would unreasonably interfere
804 with the provision of education services by or the ordinary operation of the school or institution.

805 (e) Personal data collected or processed by a controller pursuant to this section may be
806 collected or processed to the extent that such collection and processing is:

807 (1) Reasonably necessary and proportionate to the purposes listed in this section, or, in
808 the case of sensitive data, strictly necessary to the purposes listed in this section;

809 (2) limited to what is necessary in relation to the specific purposes listed in this section.

810 Personal data processed pursuant to subsection (b) of this section shall, where applicable, take
811 into account the nature and purpose or purposes of such processing. Such data shall be subject to
812 reasonable administrative, technical and physical measures to protect the confidentiality,

813 integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm
814 to consumers relating to such processing of personal data; and

815 (3) compliant with section 4, subsection (f).

816 (f) If a controller collects or processes personal data pursuant to an exemption in this
817 section, the controller bears the burden of demonstrating that such collection or processing
818 qualifies for the exemption and complies with the requirements in subsection (e) of this section.

819 Section 11. Rulemaking.

820 The Attorney General may adopt rules and regulations to implement this Act.

821 Section 12. Enforcement.

822 (a) The Attorney General may bring a civil action against a controller or processor that
823 violates this chapter to:

824 (1) Enjoin an act or practice that is in violation of this chapter;

825 (2) enforce compliance with this chapter or a rule adopted under this chapter;

826 (3) obtain damages, restitution or other compensation on behalf of the residents of the
827 Commonwealth;

828 (4) impose civil penalties in an amount not less than \$15,000 per individual per violation,
829 as adjusted annually to reflect an increase in the Consumer Price Index; or

830 (5) obtain reasonable attorney's fees and other litigation costs, including but not limited to
831 investigative costs and expert fees, reasonably incurred.

832 (b) A violation of this chapter or a rule adopted under this chapter with respect to the
833 personal data of a consumer constitutes an injury to that consumer. The injured consumer may
834 bring a civil action against the party that commits the violation, provided such party is not a
835 small business. In a civil action brought under this subsection in which a plaintiff prevails, the
836 court may award the plaintiff:

837 (1) Damages in an amount not less than \$15,000 per individual per violation, as adjusted
838 annually to reflect an increase in the Consumer Price Index, or actual damages, whichever is
839 greater;

840 (2) punitive damages;

841 (3) injunctive relief, including an order that an entity retrieve any personal data
842 transferred in violation of this title;

843 (4) declaratory relief; or

844 (5) reasonable attorney's fees and litigation costs.

845 (c) If the court finds that a defendant has engaged in flagrant, willful, and repeated
846 violations of this chapter in an action brought by the Attorney General pursuant to subsection (a)
847 of this section, the court may issue an order to suspend or prohibit the defendant from operating
848 in the commonwealth in addition to any other remedies under subsection (a) of this section.

849 (d) When calculating awards and civil penalties in any action under this section, the court
850 shall consider:

851 (1) the number of affected individuals and the amount and sensitivity of any personal data
852 at issue;

- 853 (2) the severity of the violation or noncompliance;
- 854 (3) the risks caused by the violation or noncompliance;
- 855 (4) whether the violation or noncompliance was part of a pattern of noncompliance and
856 violations and not an isolated instance;
- 857 (5) whether the violation or noncompliance was willful and not the result of error;
- 858 (6) the precautions taken by the defendant to prevent a violation;
- 859 (7) the number of administrative actions, lawsuits, settlements, and consent-decrees under
860 this chapter involving the defendant;
- 861 (8) the number of administrative actions, lawsuits, settlements, and consent-decrees
862 involving the defendant in other states and at the federal level in issues involving information
863 privacy; and
- 864 (9) the international record of the defendant when it comes to information privacy issues.
- 865 (e) A violation of the requirements of this chapter constitutes an unfair or deceptive
866 practice in the conduct of trade or commerce for the purposes of chapter 93A.
- 867 (f) Any provision of a contract or agreement of any kind, including but not limited to a
868 controller's terms of service or a privacy policy that purports to waive or limit in any way an
869 individual's rights under this chapter, including but not limited to any right to a remedy or means
870 of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.
- 871 (g) No private or government action brought pursuant to this chapter shall preclude any
872 other action under this chapter.

873 Section 13. Relationship to Other Laws

874 (a) Nothing in this chapter shall diminish any individual’s rights or obligations under
875 chapters 66A, 93A, 93H, or under sections 1B or 3B of chapter 214.

876 Section 14. Targeted Advertising to Minors

877 A controller shall not engage in targeted advertising or first-party advertising to a
878 consumer if the controller knows or willfully disregards the fact that the consumer is a minor.

879 Section 15. Additional Protections for Location Information

880 (a) With respect to precise geolocation data that reveals that an individual or a device that
881 identifies or is linked or reasonably linkable to 1 or more individuals is presently in or was in the
882 Commonwealth of Massachusetts:

883 (1) an individual shall have the same rights, privileges, and protections as a consumer
884 under this chapter for all such precise location data that is linked or reasonably linkable to that
885 individual or a device associated with that individual; and

886 (2) a controller shall treat such precise geolocation data in the same manner as it
887 would the precise geolocation data of a consumer under this chapter.

888 Section 16. Deadlines for certain actions.

889 The first data protection assessments required by section 8 are required to be completed
890 not later than the first anniversary of the effective date of this Act.

891 Section 17. Effective date.

This Act takes effect 180 days after enactment.