

HOUSE No. 83

The Commonwealth of Massachusetts

PRESENTED BY:

Andres X. Vargas and David M. Rogers

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 to establish the Massachusetts data privacy protection act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>Andres X. Vargas</i>	<i>3rd Essex</i>	<i>1/10/2023</i>
<i>David M. Rogers</i>	<i>24th Middlesex</i>	<i>1/19/2023</i>
<i>Carmin Lawrence Gentile</i>	<i>13th Middlesex</i>	<i>2/9/2023</i>
<i>Marjorie C. Decker</i>	<i>25th Middlesex</i>	<i>1/11/2024</i>
<i>Tommy Vitolo</i>	<i>15th Norfolk</i>	<i>1/23/2024</i>

HOUSE No. 83

By Representatives Vargas of Haverhill and Rogers of Cambridge, a petition (accompanied by bill, House, No. 83) of Andres X. Vargas, David M. Rogers and Carmine Lawrence Gentile for legislation to establish the Massachusetts data privacy protection act. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Third General Court
(2023-2024)**

An Act to establish the Massachusetts data privacy protection 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 SECTION 1. The General Laws, as appearing in the 2018 Official Edition, are hereby
2 amended by inserting after chapter 93K the following chapter:

3 Chapter 93L. Massachusetts Data Privacy Protection Act

4 Section 1. Definitions

5 As used in this chapter, the following words shall, unless the context clearly requires
6 otherwise, have the following meanings:—

7 “affirmative express consent”, an affirmative act by an individual that clearly
8 communicates the individual’s freely given, specific, and unambiguous authorization for an act
9 or practice after having been informed, in response to a specific request from a covered entity
10 that meets the requirements of this chapter.

11 “authentication”, the process of verifying an individual or entity for security purposes.

12 “biometric information”, any covered data generated from the technological processing
13 of an individual’s unique biological, physical, or physiological characteristics that is linked or
14 reasonably linkable to an individual, including:—

15 fingerprints;

16 voice prints;

17 iris or retina scans;

18 facial or hand mapping, geometry, or templates; or

19 gait or personally identifying physical movements.

20 The term “biometric information” does not include a digital or physical photograph; an
21 audio or video recording; or data generated from a digital or physical photograph, or an audio or
22 video recording, that cannot be used to identify an individual.

23 “collect” and “collection”, buying, renting, gathering, obtaining, receiving, accessing, or
24 otherwise acquiring covered data by any means.

25 “control”, with respect to an entity:—

26 ownership of, or the power to vote, more than 50 percent of the outstanding shares of any
27 class of voting security of the entity;

28 control over the election of a majority of the directors of the entity (or of individuals
29 exercising similar functions); or

30 the power to exercise a controlling influence over the management of the entity.

31 “covered algorithm”, a computational process that uses machine learning, natural
32 language processing, artificial intelligence techniques, or other computational processing
33 techniques of similar or greater complexity and that makes a decision or facilitates human
34 decision-making with respect to covered data, including determining the provision of products or
35 services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or
36 display of information to an individual.

37 “covered data”, information, including derived data and unique persistent identifiers, that
38 identifies or is linked or reasonably linkable, alone or in combination with other information, to
39 an individual or a device that identifies or is linked or reasonably linkable to an individual. The
40 term “covered data” does not include:—

41 de-identified data;

42 employee data covered under section 204 of chapter 149 of the general laws; or

43 publicly available information.

44 “covered entity”, any entity or any person, other than an individual acting in a non-
45 commercial context, that alone or jointly with others determines the purposes and means of
46 collecting, processing, or transferring covered data. The term “covered entity” does not
47 include:—

48 government agencies or service providers to government agencies that exclusively and
49 solely process information provided by government entities;

50 any entity or person that meets the following criteria for the period of the 3 preceding
51 calendar years (or for the period during which the covered entity or service provider has been in
52 existence if such period is less than 3 years):—

53 the entity or person’s average annual gross revenues during the period did not exceed
54 \$20,000,000;

55 the entity or person, on average, did not annually collect or process the covered data of
56 more than 75,000 individuals during the period beyond the purpose of initiating, rendering,
57 billing for, finalizing, completing, or otherwise collecting payment for a requested service or
58 product, so long as all covered data for such purpose was deleted or de-identified within 90 days,
59 except when necessary to investigate fraud or as consistent with a covered entity’s return policy;
60 and

61 no component of its revenue comes from transferring covered data during any year (or
62 part of a year if the covered entity has been in existence for less than 1 year) that occurs during
63 the period.

64 “covered high-impact social media company”, a covered entity that provides any internet-
65 accessible platform where—

66 such covered entity generates \$3,000,000,000 or more in annual revenue;

67 such platform has 300,000,000 or more monthly active users for not fewer than 3 of the
68 preceding 12 months on the online product or service of such covered entity; and

69 such platform constitutes an online product or service that is primarily used by users to
70 access or share, user-generated content.

71 “covered minor”, an individual under the age of 18.

72 “de-identified data”, information that does not identify and is not linked or reasonably
73 linkable to a distinct individual or a device, regardless of whether the information is aggregated,
74 and if the covered entity or service provider:—

75 takes technical measures to ensure that the information cannot, at any point, be used to
76 re-identify any individual or device that identifies or is linked or reasonably linkable to an
77 individual;

78 publicly commits in a clear and conspicuous manner:—

79 to process and transfer the information solely in a de-identified form without any
80 reasonable means for re-identification; and

81 to not attempt to re-identify the information with any individual or device that identifies
82 or is linked or reasonably linkable to an individual; and

83 contractually obligates any person or entity that receives the information from the
84 covered entity or service provider:—

85 to comply with all the provisions of this paragraph with respect to the information; and

86 to require that such contractual obligations be included contractually in all subsequent
87 instances for which the data may be received.

88 “derived data”, covered data that is created by the derivation of information, data,
89 assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another
90 source of information or data about an individual or an individual’s device.

91 “device”, any electronic equipment capable of collecting, processing, or transferring data
92 that is used by one or more individuals or households.

93 “first party advertising or marketing”, advertising or marketing conducted by a covered
94 entity that collected covered data from the individual through either direct communications with
95 the individual such as direct mail, email, or text message communications, or advertising or
96 marketing conducted entirely within the first-party context, such as in a physical location
97 operated by or on behalf of such covered entity, or on a web site or app operated by or on behalf
98 of such covered entity.

99 “genetic information”, any covered data, regardless of its format, that concerns an
100 individual’s genetic characteristics, including:—

101 raw sequence data that results from the sequencing of the complete, or a portion of the,
102 extracted deoxyribonucleic acid (DNA) of an individual; or

103 genotypic and phenotypic information that results from analyzing raw sequence data
104 described in subparagraph (A).

105 “individual”, a natural person who is a Massachusetts resident or present in
106 Massachusetts.

107 “knowledge”,

108 with respect to a covered entity that is a covered high-impact social media company, the
109 entity knew or should have known the individual was a covered minor;

110 with respect to a covered entity or service provider that is a large data holder, and
111 otherwise is not a covered high-impact social media company, that the covered entity knew or
112 acted in willful disregard of the fact that the individual was a covered minor; and

113 with respect to a covered entity or service provider that does not meet the requirements of
114 clause (i) or (ii), actual knowledge.

115 “large data holder”, a covered entity or service provider that in the most recent calendar
116 year:—

117 had annual gross revenues of \$250,000,000 or more; and

118 collected, processed, or transferred the covered data of more than 5,000,000 individuals
119 or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding
120 covered data collected and processed solely for the purpose of initiating, rendering, billing for,
121 finalizing, completing, or otherwise collecting payment for a requested product or service; and
122 the sensitive covered data of more than 200,000 individuals or devices that identify or are linked
123 or reasonably linkable to 1 or more individuals.

124 The term “large data holder” does not include any instance in which the covered entity or
125 service provider would qualify as a large data holder solely on the basis of collecting or
126 processing personal email addresses, personal telephone numbers, or log-in information of an
127 individual or device to allow the individual or device to log in to an account administered by the
128 covered entity or service provider.

129 “material”, with respect to an act, practice, or representation of a covered entity
130 (including a representation made by the covered entity in a privacy policy or similar disclosure to

131 individuals) involving the collection, processing, or transfer of covered data, that such act,
132 practice, or representation is likely to affect a reasonable individual’s decision or conduct
133 regarding a product or service;

134 “location information”, information derived from a device or from interactions between
135 devices, with or without the knowledge of the user and regardless of the technological method
136 used, that pertains to or directly or indirectly reveals the present or past geographical location of
137 an individual or device within the Commonwealth of Massachusetts with sufficient precision to
138 identify street-level location information within a range of 1,850 feet or less.

139 “OCABR”, the Office of Consumer Affairs and Business Regulation.

140 “process”, to conduct or direct any operation or set of operations performed on covered
141 data, including analyzing, organizing, structuring, retaining, storing, using, or otherwise handling
142 covered data.

143 “processing purpose”, a reason for which a covered entity or service provider collects,
144 processes, or transfers covered data that is specific and granular enough for a reasonable
145 individual to understand the material facts of how and why the covered entity or service provider
146 collects, processes, or transfers the covered data.

147 “publicly available information”, any information that a covered entity or service
148 provider has a reasonable basis to believe has been lawfully made available to the general public
149 from:—

150 federal, state, or local government records, if the covered entity collects, processes, and
151 transfers such information in accordance with any restrictions or terms of use placed on the
152 information by the relevant government entity;

153 widely distributed media;

154 a website or online service made available to all members of the public, for free or for a
155 fee, including where all members of the public, for free or for a fee, can log in to the website or
156 online service;

157 a disclosure that has been made to the general public as required by federal, state, or local
158 law; or

159 the visual observation of the physical presence of an individual or a device in a public
160 place, not including data collected by a device in the individual's possession.

161 For purposes of this paragraph, information from a website or online service is not
162 available to all members of the public if the individual who made the information available via
163 the website or online service has restricted the information to a specific audience.

164 The term "publicly available information" does not include:—

165 any obscene visual depiction, as defined in section 18 U.S.C. section 1460;

166 any inference made exclusively from multiple independent sources of publicly available
167 information that reveals sensitive

168 covered data with respect to an individual;

169 biometric information;

170 publicly available information that has been combined with covered data;

171 genetic information, unless otherwise made available by the individual to whom the
172 information pertains;

173 intimate images known to have been created or shared without consent..

174 “reasonably understandable”, of length and complexity such that an individual with an
175 eighth-grade reading level, as established by the department of elementary and secondary
176 education, can read and comprehend.

177 “sensitive covered data”, the following types of covered data:—

178 a government-issued identifier, such as a Social Security number, passport number, or
179 driver’s license number, that is not required by law to be displayed in public.

180 any information that describes or reveals the past, present, or future physical health,
181 mental health, disability, diagnosis, or healthcare condition or treatment of an individual.

182 a financial account number, debit card number, credit card number, or information that
183 describes or reveals the income level or bank account balances of an individual, except that the
184 last four digits of a debit or credit card number shall not be deemed sensitive covered data.

185 biometric information.

186 genetic information.

187 location information.

188 an individual's private communications such as voicemails, emails, texts, direct
189 messages, or mail, or information identifying the parties to such communications, voice
190 communications, video communications, and any information that pertains to the transmission of
191 such communications, including telephone numbers called, telephone numbers from which calls
192 were placed, the time calls were made, call duration, and location information of the parties to
193 the call, unless the covered entity or a service provider acting on behalf of the covered entity is
194 the sender or an intended recipient of the communication. Communications are not private for
195 purposes of this clause if such communications are made from or to a device provided by an
196 employer to an employee insofar as such employer provides conspicuous notice that such
197 employer may access such communications.

198 account or device log-in credentials, or security or access codes for an account or device.

199 information identifying the sexual behavior of an individual in a manner inconsistent with
200 the individual's reasonable expectation regarding the collection, processing, or transfer of such
201 information or when it is processed in a way that creates a substantial privacy risk for the
202 individual.

203 calendar information, address book information, phone or text logs, photos, audio
204 recordings, or videos, maintained for private use by an individual, regardless of whether such
205 information is stored on the individual's device or is accessible from that device and is backed up
206 in a separate location. Such information is not sensitive for purposes of this paragraph if such
207 information is sent from or to a device provided by an employer to an employee insofar as such
208 employer provides conspicuous notice that it may access such information.

209 a photograph, film, video recording, or other similar medium that shows the naked or
210 undergarment-clad private area of an individual.

211 information revealing the video content requested or selected by an individual collected
212 by a covered entity that is not a provider of a service described in section 102(4). This clause
213 does not include covered data used solely for transfers for independent video measurement.

214 information about an individual when the covered entity or service provider has
215 knowledge that the individual is a covered minor.

216 an individual's race, color, ethnicity, sex, gender identity, sexual orientation, national
217 origin, immigration status, disability, religion, or union membership.

218 information identifying an individual's online activities over time and across third-party
219 websites or online services.

220 any other covered data collected, processed, or transferred for the purpose of identifying
221 the types of covered data listed in clauses (1) through (16).

222 "service provider", a person or entity that:—

223 collects, processes, or transfers covered data on behalf of, and at the direction of, a
224 covered entity or a government agency; and

225 receives covered data from or on behalf of a covered entity or a government agency.

226 A service provider that receives service provider data from another service provider as
227 permitted under this chapter shall be treated as a service provider under this chapter with respect
228 to such data.

229 “service provider data”, covered data that is collected or processed by or has been
230 transferred to a service provider by or on behalf of a covered entity or a government agency or
231 another service provider for the purpose of allowing the service provider to whom such covered
232 data is transferred to perform a service or function on behalf of, and at the direction of, such
233 covered entity or government agency.

234 “small business”, a covered entity or a service provider that meets the following criteria
235 for the period of the 3 preceding calendar years (or for the period during which the covered
236 entity or service provider has been in existence if such period is less than 3 years):—

237 the covered entity or service provider’s average annual gross revenues during the period
238 did not exceed \$41,000,000;

239 the covered entity or service provider, on average, did not annually collect or process the
240 covered data of more than 200,000 individuals during the period beyond the purpose of
241 initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a
242 requested service or product, so long as all covered data for such purpose was deleted or de-
243 identified within 90 days, except when necessary to investigate fraud or as consistent with a
244 covered entity’s return policy; and

245 the covered entity or service provider did not derive more than 50 percent of its revenue
246 from transferring covered data during any year (or part of a year if the covered entity has been in
247 existence for less than 1 year) that occurs during the period.

248 “substantial privacy risk”, the collection, processing, or transfer of covered data in a
249 manner that may result in any reasonably foreseeable substantial physical injury, economic
250 injury, highly offensive intrusion into the privacy expectations of a reasonable individual under

251 the circumstances, or discrimination on the basis of race, color, religion, national origin, sex,
252 sexual orientation, gender identity or disability.

253 “targeted advertising”, presenting to an individual or device identified by a unique
254 identifier, or groups of individuals or devices identified by unique identifiers, an online
255 advertisement that is selected based on known or predicted preferences, characteristics, or
256 interests associated with the individual or a device identified by a unique identifier; and does not
257 include:—

258 advertising or marketing to an individual or an individual’s device in response to the
259 individual’s specific request for information or feedback;

260 contextual advertising, which is when an advertisement is displayed based on the content
261 in which the advertisement appears and does not vary based on who is viewing the
262 advertisement; or

263 processing covered data solely for measuring or reporting advertising or content,
264 performance, reach, or frequency, including independent measurement.

265 “third party”, any person or entity, including a covered entity, that—

266 collects, processes, or transfers covered data and is not a consumer-facing business with
267 which the individual linked or reasonably linkable to such covered data expects and intends to
268 interact; and

269 is not a service provider with respect to such data.

270 This term does not include a person or entity that collects covered data from another
271 entity if the two entities are related by common ownership or corporate control, but only if a
272 reasonable consumer’s reasonable expectation would be that such entities share information.

273 “data broker”, a covered entity whose principal source of revenue is derived from
274 processing or transferring covered data that the covered entity did not collect directly from the
275 individuals linked or linkable to the covered data. This term does not include a covered entity
276 insofar as such entity processes employee data collected by and received from a third party
277 concerning any individual who is an employee of the third party for the sole purpose of such
278 third-party providing benefits to the employee. An entity may not be considered to be a data
279 broker for purposes of this chapter if the entity is acting as a service provider.

280 “third party data”, covered data that has been transferred to a third party.

281 “transfer”, to disclose, release, disseminate, make available, license, rent, or share
282 covered data orally, in writing, electronically, or by any other means.

283 “unique identifier”, an identifier to the extent that such identifier is reasonably linkable to
284 an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals,
285 including a device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad
286 identifier, or similar technology, customer number, unique pseudonym, user alias, telephone
287 number, or other form of persistent or probabilistic identifier that is linked or reasonably linkable
288 to an individual or device. This term does not include an identifier assigned by a covered entity
289 for the specific purpose of giving effect to an individual’s exercise of affirmative express consent
290 or opt-outs of the collection, processing, and transfer of covered data pursuant to this chapter or
291 otherwise limiting the collection, processing, or transfer of such information.

292 “widely distributed media”, information that is available to the general public, including
293 information from a telephone book or online directory, a television, internet, or radio program,
294 the news media, or an internet site that is available to the general public on an unrestricted basis,
295 but does not include an obscene visual depiction, as defined in 18 U.S.C. section 1460.

296 Section 2. Duty of Loyalty

297 A covered entity may not collect, process, or transfer covered data unless the collection,
298 processing, or transfer is limited to what is reasonably necessary and proportionate to carry out
299 one of the following purposes:—

300 provide or maintain a specific product or service requested by the individual to whom the
301 data pertains;

302 initiate, manage, complete a transaction, or fulfill an order for specific products or
303 services requested by an individual, including any associated routine administrative, operational,
304 and account-servicing activity such as billing, shipping, delivery, storage, and accounting;

305 authenticate users of a product or service;

306 fulfill a product or service warranty;

307 prevent, detect, protect against, or respond to a security incident. For purposes of this
308 paragraph, security is defined as network security and physical security and life safety, including
309 an intrusion or trespass, medical alerts, fire alarms, and access control security;

310 to prevent, detect, protect against, or respond to fraud, harassment, or illegal activity
311 targeted at or involving the covered entity or its services. For purposes of this paragraph, the

312 term “illegal activity”, a violation of a federal, state, or local law punishable as a felony or
313 misdemeanor that can directly harm;

314 comply with a legal obligation imposed by state or federal law, or to investigate,
315 establish, prepare for, exercise, or defend legal claims involving the covered entity or service
316 provider;

317 effectuate a product recall pursuant to state or federal law;

318 conduct a public or peer-reviewed scientific, historical, or statistical research project
319 that:—

320 is in the public interest; and

321 adheres to all relevant laws and regulations governing such research, including
322 regulations for the protection of human subjects, or is excluded from criteria of the institutional
323 review board;

324 deliver a communication that is not an advertisement to an individual, if the
325 communication is reasonably anticipated by the individual within the context of the individual’s
326 interactions with the covered entity;

327 deliver a communication at the direction of an individual between such individual and
328 one or more individuals or entities;

329 ensure the data security and integrity of covered data in accordance with chapter 93H;

330 to support or promote participation by individuals in civic engagement activities and
331 democratic governance, including voting, petitioning, engaging with government proceedings,
332 providing indigent legal aid services, and unionizing; or

333 transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or
334 similar transaction when the third party assumes control, in whole or in part, of the covered
335 entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides
336 each affected individual with:—

337 a notice describing such transfer, including the name of the entity or entities receiving the
338 individual's covered data and their privacy policies; and

339 a reasonable opportunity to withdraw any previously given consents related to the
340 individual's covered data and a reasonable opportunity to request the deletion of the individual's
341 covered data.

342 A covered entity may, with respect to covered data previously collected in accordance
343 with the previous subsection, process such data:—

344 as necessary to provide first-party advertising or marketing of products or services
345 provided by the covered entity for individuals who are not covered minors;

346 to provide targeted advertising; provided, however, that such collection, processing, and
347 transferring complies with the requirements of this chapter;

348 process such data as necessary to perform system maintenance or diagnostics;

349 develop, maintain, repair, or enhance a product or service for which such data was
350 collected;

351 to conduct internal research or analytics to improve a product or service for which such
352 data was collected;
353 perform inventory management or reasonable network management;
354 protect against spam; or
355 debug or repair errors that impair the functionality of a service or product for which such
356 data was collected.

357 A covered entity or service provider shall not:—
358 engage in deceptive advertising or marketing with respect to a product or service offered
359 to an individual; or
360 draw an individual into signing up for or acquiring a product or service through:—
361 the use of any false, fictitious, fraudulent, or materially misleading statement or
362 representation; or
363 the design, modification, or manipulation of any user interface with the purpose or
364 substantial effect of obscuring, subverting, or impairing a reasonable individual’s autonomy,
365 decision-making, or choice.

366 Nothing in this chapter shall be construed or interpreted to:—
367 limit or diminish free speech rights of covered entities guaranteed under the First
368 Amendment to the Constitution of the United States or under Article 16 of Massachusetts
369 Declaration of Rights; or

370 imply any purpose that is not enumerated in subsections (a) and (b), when applicable.

371 Section 3. Sensitive covered data.

372 A covered entity or service provider shall not:—

373 collect, process, or transfer a Social Security number, except when necessary to facilitate
374 an extension of credit, authentication, fraud and identity fraud detection and prevention, the
375 payment or collection of taxes, the enforcement of a contract between parties, or the prevention,
376 investigation, or prosecution of fraud or illegal activity, or as otherwise required by state or
377 federal law;

378 collect or process sensitive covered data, except where such collection or processing is
379 strictly necessary to provide or maintain a specific product or service requested by the individual
380 to whom the covered data pertains or is strictly necessary to effect a purpose enumerated in
381 paragraphs (1), (2), (3), (5), (7), (9), (10), (11), (13), (14) of subsection (a) of section 2, and such
382 data is only used for that purposes;

383 transfer an individual's sensitive covered data to a third party, unless:—

384 the transfer is made pursuant to the affirmative express consent of the individual, given
385 before each specific transfer takes place;

386 the transfer is necessary to comply with a legal obligation imposed by state or federal
387 law, so long as such obligation preexisted the collection and previous notice of such obligation
388 was provided to the individual to whom the data pertains;

389 the transfer is necessary to prevent an individual from imminent injury where the covered
390 entity believes in good faith that the individual is at risk of death, serious physical injury, or
391 serious health risk;

392 in the case of the transfer of a password, the transfer is necessary to use a designated
393 password manager or is to a covered entity for the exclusive purpose of identifying passwords
394 that are being re-used across sites or accounts;

395 in the case of the transfer of genetic information, the transfer is necessary to perform a
396 medical diagnosis or medical treatment specifically requested by an individual, or to conduct
397 medical research in accordance with federal and state law; and

398 in the case of transfer assets in case of a merger, if the transfer is made in accordance
399 with paragraph (14) of subsection (a) of section (2); or

400 process sensitive covered data for purposes of targeted advertising.

401 Section 4. Consent practices

402 The requirements of this chapter with respect to a request for affirmative consent from a
403 covered entity to an individual are the following:—

404 The request for affirmative consent should be provided to the individual in a clear and
405 conspicuous standalone disclosure made through the primary medium used to offer the covered
406 entity's product or service, or only if the product or service is not offered in a medium that
407 permits the making of the request under this paragraph, another medium regularly used in
408 conjunction with the covered entity's product or service;

409 The request includes a description of the processing purpose for which the individual's
410 consent is sought by:—

411 clearly stating the specific categories of covered data that the covered entity shall collect,
412 process, and transfer necessary to effectuate the processing purpose; and

413 including a prominent heading and is reasonably understandable so that an individual can
414 identify and understand the processing purpose for which consent is sought and the covered data
415 to be collected, processed, or transferred by the covered entity for such processing purpose;

416 The request clearly explains the individual's applicable rights related to consent;

417 The request is made in a manner reasonably accessible to and usable by individuals with
418 disabilities;

419 The request is made available to the individual in each covered language in which the
420 covered entity provides a product or service for which authorization is sought;

421 The option to refuse consent shall be at least as prominent as the option to accept, and the
422 option to refuse consent shall take the same number of steps or fewer as the option to accept; and

423 Processing or transferring any covered data collected pursuant to affirmative express
424 consent for a different processing purpose than that for which affirmative express consent was
425 obtained shall require affirmative express consent for the subsequent processing purpose.

426 A covered entity shall not infer that an individual has provided affirmative express
427 consent to a practice from the inaction of the individual or the individual's continued use of a
428 service or product provided by the covered entity.

429 A covered entity shall not obtain or attempt to obtain the affirmative express consent of
430 an individual through:—

431 the use of any false, fictitious, fraudulent, or materially misleading statement or
432 representation; or

433 the design, modification, or manipulation of any user interface with the purpose or
434 substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy,
435 decision-making, or choice to provide such consent or any covered data.

436 Section 5. Privacy by design

437 A covered entity and a service provider shall establish, implement, and maintain
438 reasonable policies, practices, and procedures that reflect the role of the covered entity or service
439 provider in the collection, processing, and transferring of covered data and that:—

440 consider applicable federal and state laws, rules, or regulations related to covered data the
441 covered entity or service provider collects, processes, or transfers;

442 identify, assess, and mitigate privacy risks related to covered minors;

443 mitigate privacy risks, including substantial privacy risks, related to the products and
444 services of the covered entity or the service provider, including in the design, development, and
445 implementation of such products and services, considering the role of the covered entity or
446 service provider and the information available to it; and

447 implement reasonable training and safeguards within the covered entity and service
448 provider to promote compliance with all privacy laws applicable to covered data the covered
449 entity collects, processes, or transfers or covered data the service provider collects, processes, or

450 transfers on behalf of the covered entity and mitigate privacy risks, including substantial privacy
451 risks, taking into account the role of the covered entity or service provider and the information
452 available to it.

453 The policies, practices, and procedures established by a covered entity and a service
454 provider under subsection (a), shall correspond with, as applicable:—

455 the size of the covered entity or the service provider and the nature, scope, and
456 complexity of the activities engaged in by the covered entity or service provider, including
457 whether the covered entity or service provider is a large data holder, nonprofit organization,
458 small business, third party, or data broker, considering the role of the covered entity or service
459 provider and the information available to it;

460 the sensitivity of the covered data collected, processed, or transferred by the covered
461 entity or service provider;

462 the volume of covered data collected, processed, or transferred by the covered entity or
463 service provider;

464 the number of individuals and devices to which the covered data collected, processed, or
465 transferred by the covered entity or service provider relates; and

466 the cost of implementing such policies, practices, and procedures in relation to the risks
467 and nature of the covered data.

468 Section 6. Pricing

469 A covered entity may not retaliate against an individual for:—

470 exercising any of the rights guaranteed by this chapter, or any regulations promulgated
471 under this chapter; or

472 refusing to agree to collection or processing of covered data for a separate product or
473 service, including denying goods or services, charging different prices or rates for goods or
474 services, or providing a different level of quality of goods or services.

475 Nothing in subsection (a) shall be construed to:—

476 prohibit the relation of the price of a service or the level of service provided to an
477 individual to the provision, by the individual, of financial information that is necessarily
478 collected and processed only for the purpose of initiating, rendering, billing for, or collecting
479 payment for a service or product requested by the individual;

480 prohibit a covered entity from offering a different price, rate, level, quality or selection of
481 goods or services to an individual, including offering goods or services for no fee, if the offering
482 is in connection with an individual's voluntary participation in a bona fide loyalty, , rewards,
483 premium features, discount or club card program, provided, that the covered entity may not sell
484 covered data to a third-party as part of such a program unless:—

485 the sale is reasonably necessary to enable the third party to provide a benefit to which the
486 consumer is entitled;

487 the sale of personal data to third parties is clearly disclosed in the terms of the program;

488 and

489 the third party uses the personal data only for purposes of facilitating such a benefit to
490 which the consumer is entitled and does not retain or otherwise use or disclose the personal data
491 for any other purpose;

492 require a covered entity to provide a bona fide loyalty program that would require the
493 covered entity to collect, process, or transfer covered data that the covered entity otherwise
494 would not collect, process, or transfer;

495 prohibit a covered entity from offering a financial incentive or other consideration to an
496 individual for participation in market research;

497 prohibit a covered entity from offering different types of pricing or functionalities with
498 respect to a product or service based on an individual's exercise of a right to delete; or

499 prohibit a covered entity from declining to provide a product or service insofar as the
500 collection and processing of covered data is strictly necessary for such product or service.

501 Notwithstanding the provisions in this subsection, no covered entity may offer
502 different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

503 Section 7. Privacy policy

504 Each covered entity and service provider shall make publicly available, in a clear,
505 conspicuous, not misleading, a reasonably understandable privacy policy that provides a detailed
506 and accurate representation of the data collection, processing, and transfer activities of the
507 covered entity.

508 The privacy policy must be provided in a manner that is reasonably accessible to and
509 usable by individuals with disabilities. The policy shall be made available to the public in each

510 covered language in which the covered entity or service provider provides a product or service
511 that is subject to the privacy policy; or carries out activities related to such product or service.

512 The privacy policy must include, at a minimum, the following:—

513 The identity and the contact information of:—

514 the covered entity or service provider to which the privacy policy applies, including the
515 covered entity's or service provider's points of contact and generic electronic mail addresses, as
516 applicable for privacy and data security inquiries;

517 any other entity within the same corporate structure as the covered entity or service
518 provider to which covered data is transferred by the covered entity;

519 the categories of covered data the covered entity or service provider collects or processes;

520 the processing purposes for each category of covered data the covered entity or service
521 provider collects or processes;

522 whether the covered entity or service provider transfers covered data and, if so, each
523 category of service provider and third party to which the covered entity or service provider
524 transfers covered data, the name of each data broker to which the covered entity or service
525 provider transfers covered data, and the purposes for which such data is transferred to such
526 categories of service providers and third parties or third-party collecting entities, except for a
527 transfer to a governmental entity pursuant to a court order or law that prohibits the covered entity
528 or service provider from disclosing such transfer;

529 The length of time the covered entity or service provider intends to retain each category
530 of covered data, including sensitive covered data, or, if it is not possible to identify that

531 timeframe, the criteria used to determine the length of time the covered entity or service provider
532 intends to retain categories of covered data;

533 A prominent description of how an individual can exercise the rights described in this
534 chapter;

535 A general description of the covered entity's or service provider's data security practices;
536 and

537 The effective date of the privacy policy.

538 If a covered entity makes a material change to its privacy policy or practices, the covered
539 entity shall notify each individual affected by such material change before implementing the
540 material change with respect to any prospectively collected covered data and, except as provided
541 in paragraphs (1) through (15) of section 2, provide a reasonable opportunity for each individual
542 to withdraw consent to any further materially different collection, processing, or transfer of
543 previously collected covered data under the changed policy.

544 The covered entity shall take all reasonable electronic measures to provide direct
545 notification regarding material changes to the privacy policy to each affected individual, in each
546 covered language in which the privacy policy is made available, and taking into account
547 available technology and the nature of the relationship.

548 Nothing in this section shall be construed to affect the requirements for covered entities
549 under other sections of this chapter.

550 Each large data holder shall retain copies of previous versions of its privacy policy for at
551 least 10 years beginning after the date of enactment of this chapter and publish them on its

552 website. Such large data holder shall make publicly available, in a clear, conspicuous, and
553 readily accessible manner, a log describing the date and nature of each material change to its
554 privacy policy over the past 10 years. The descriptions shall be sufficient for a reasonable
555 individual to understand the material effect of each material change. The obligations in this
556 paragraph shall not apply to any previous versions of a large data holder’s privacy policy, or any
557 material changes to such policy, that precede the date of enactment of this Act.

558 In addition to the privacy policy required under subsection (a), a large data holder that is
559 a covered entity shall provide a short form notice of no more than 500 words in length that
560 includes the main features of their data practices.

561 Section 8. Individual data rights

562 A covered entity shall provide an individual, after receiving a verified request from the
563 individual, with the right to:—

564 access:—

565 in a human-readable format that a reasonable individual can understand and download
566 from the internet, the covered data (except covered data in a back-up or archival system) of the
567 individual making the request that is collected, processed, or transferred by the covered entity or
568 any service provider of the covered entity within the 24 months preceding the request;

569 the categories of any third party, if applicable, and an option for consumers to obtain the
570 names of any such third party as well as and the categories of any service providers to whom the
571 covered entity has transferred for consideration the covered data of the individual, as well as the
572 categories of sources from which the covered data was collected; and

573 a description of the purpose for which the covered entity transferred the covered data of
574 the individual to a third party or service provider;

575 correct any verifiable substantial inaccuracy or substantially incomplete information with
576 respect to the covered data of the individual that is processed by the covered entity and instruct
577 the covered entity to make reasonable efforts to notify all third parties or service providers to
578 which the covered entity transferred such covered data of the corrected information;

579 delete covered data of the individual that is processed by the covered entity and instruct
580 the covered entity to make reasonable efforts to notify all third parties or service provider to
581 which the covered entity transferred such covered data of the individual's deletion request; and

582 to the extent technically feasible, export to the individual or directly to another entity the
583 covered data of the individual that is processed by the covered entity, including inferences linked
584 or reasonably linkable to the individual but not including other derived data, without licensing
585 restrictions that limit such transfers in:—

586 a human-readable format that a reasonable individual can understand and download from
587 the internet; and

588 a portable, structured, interoperable, and machine-readable format.

589 A covered entity may not condition, effectively condition, attempt to condition, or
590 attempt to effectively condition the exercise of a right described in subsection (a) through:—

591 the use of any false, fictitious, fraudulent, or materially misleading statement or
592 representation; or

593 the design, modification, or manipulation of any user interface with the purpose or
594 substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy,
595 decision making, or choice to exercise such right.

596 Subject to subsections (d) and (e), each request under subsection (a) shall be completed
597 within 30 days of such request from an individual, unless it is demonstrably impracticable or
598 impracticably costly to verify such individual.

599 A response period set forth in this subsection may be extended once by 20 additional
600 days when reasonably necessary, considering the complexity and number of the individual's
601 requests, so long as the covered entity informs the individual of any such extension within the
602 initial 30-day response period, together with the reason for the extension.

603 A covered entity:—

604 shall provide an individual with the opportunity to exercise each of the rights described in
605 subsection (a) and with respect to:—

606 the first two times that an individual exercises any right described in subsection (a) in any
607 12-month period, shall allow the individual to exercise such right free of charge; and

608 any time beyond the initial two times described in subparagraph (A), may allow the
609 individual to exercise such right for a reasonable fee for each request.

610 A covered entity may not permit an individual to exercise a right described in subsection
611 (a), in whole or in part, if the covered entity:—

612 cannot reasonably verify that the individual making the request to exercise the right is the
613 individual whose covered data is the subject of the request or an individual authorized to make
614 such a request on the individual's behalf;

615 reasonably believes that the request is made to interfere with a contract between the
616 covered entity and another individual;

617 determines that the exercise of the right would require access to or correction of another
618 individual's sensitive covered data;

619 reasonably believes that the exercise of the right would require the covered entity to
620 engage in an unfair or deceptive practice under state law; or

621 reasonably believes that the request is made to further fraud, support criminal activity, or
622 the exercise of the right presents a data security threat.

623 If a covered entity cannot reasonably verify that a request to exercise a right described in
624 subsection (a) is made by the individual whose covered data is the subject of the request (or an
625 individual authorized to make such a request on the individual's behalf), the covered entity:—

626 may request that the individual making the request to exercise the right provide any
627 additional information necessary for the sole purpose of verifying the identity of the individual;
628 and

629 may not process or transfer such additional information for any other purpose.

630 A covered entity may decline, with adequate explanation to the individual, to comply
631 with a request to exercise a right described in subsection (a), in whole or in part, that would:—

632 require the covered entity to retain any covered data collected for a single, one-time
633 transaction, if such covered data is not processed or transferred by the covered entity for any
634 purpose other than completing such transaction;

635 be demonstrably impracticable or prohibitively costly to comply with, and the covered
636 entity shall provide a description to the requestor detailing the inability to comply with the
637 request;

638 require the covered entity to attempt to re-identify de-identified data;

639 require the covered entity to maintain covered data in an identifiable form or collect,
640 retain, or access any data in order to be capable of associating a verified individual request with
641 covered data of such individual;

642 result in the release of trade secrets or other privileged or confidential business
643 information;

644 require the covered entity to correct any covered data that cannot be reasonably verified
645 as being inaccurate or incomplete;

646 interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts
647 to guard against, detect, prevent, or investigate fraudulent, malicious, or unlawful activity, or
648 enforce valid contracts;

649 violate state or federal law or the rights and freedoms of another individual, including
650 under the Constitution of the United States and Massachusetts Declaration of Rights;

651 prevent a covered entity from being able to maintain a confidential record of deletion
652 requests, maintained solely for the purpose of preventing covered data of an individual from

653 being recollected after the individual submitted a deletion request and requested that the covered
654 entity no longer collect, process, or transfer such data; or

655 endanger the source of the data if such data could only have been obtained from a single
656 identified source.

657 A covered entity may decline, with adequate explanation to the individual, to comply
658 with a request for deletion pursuant to paragraph (3) of subsection (a) if such request:—

659 unreasonably interfere with the provision of products or services by the covered entity to
660 another person it currently serves;

661 requests to delete covered data that relates to (A) a public figure, public official, or
662 limited-purpose public figure; or (B) any other individual that has no reasonable expectation of
663 privacy with respect to such data;

664 requests to delete covered data reasonably necessary to perform a contract between the
665 covered entity and the individual;

666 requests to delete covered data that the covered entity needs to retain in order to comply
667 with professional ethical obligations;

668 requests to delete covered data that the covered entity reasonably believes may be
669 evidence of unlawful activity or an abuse of the covered entity’s products or service; or

670 involves private elementary and secondary schools as defined by state law and private
671 institutions of higher education as defined by title I of the Higher Education Act of 1965 and
672 targets covered data that would unreasonably interfere with the provision of education services
673 by or the ordinary operation of the school or institution.

674 In a circumstance that would allow a denial pursuant to this section, a covered entity shall
675 partially comply with the remainder of the request if it is possible and not unduly burdensome to
676 do so.

677 The receipt of a large number of verified requests, on its own, may not be considered to
678 render compliance with a request demonstrably impracticable.

679 A covered entity shall facilitate the ability of individuals to make requests under
680 subsection (a) in any covered language in which the covered entity provides a product or service.
681 The mechanisms by which a covered entity enables individuals to make requests under
682 subsection (a) shall be readily accessible and usable by individuals with disabilities.

683 Section 9. Advanced data rights.

684 Covered entities shall provide an individual with a clear and conspicuous, easy-to-
685 execute means to withdraw affirmative express consent. Those means shall be as easy to execute
686 by a reasonable individual as the means to provide consent.

687 Right to opt-out of covered data transfers. A covered entity:—

688 may not transfer or direct the transfer of the covered data of an individual to a third party
689 if the individual objects to the transfer; and

690 shall allow an individual to object to such a transfer through an opt out mechanism, as
691 described in section 12.

692 Right to opt out of targeted advertising. A covered entity or service provider that directly
693 delivers a targeted advertisement shall:—

694 prior to engaging in targeted advertising to an individual or device and at all times,
695 thereafter, provide such individual with a clear and conspicuous means to opt out of targeted
696 advertising;

697 abide by any opt-out designation by an individual with respect to targeted advertising and
698 notify the covered entity that directed the service provider to deliver the targeted advertisement
699 of the opt-out decision; and

700 allow an individual to make an opt-out designation with respect to targeted advertising
701 through an opt-out mechanism.

702 A covered entity or service provider that receives an opt-out notification pursuant to this
703 section shall abide by such opt-out designations by an individual and notify any other person that
704 directed the covered entity or service provider to serve, deliver, or otherwise handle the
705 advertisement of the opt-out decision.

706 A covered entity may not condition, effectively condition, attempt to condition, or
707 attempt to effectively condition the exercise of any individual right under this section through:—
708 the use of any false, fictitious, fraudulent, or materially misleading statement or
709 representation; or

710 the design, modification, or manipulation of any user interface with the purpose or
711 substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy,
712 decision making, or choice to exercise any such right.

713 A covered entity shall notify third parties who had access to an individual's covered data
714 when the individual exercises any of the rights established in this section. The third party shall

715 comply with the request to opt-out of sale or data transfer forwarded to them from a covered
716 entity that provided, made available, or authorized the collection of the individual's covered data.
717 The third party shall comply with the request in the same way a covered entity is required to
718 comply with the request. The third party shall no longer retain, use, or disclose the personal
719 information unless the third party becomes a service provider or a covered entity in the terms of
720 this chapter.

721 Section 10. Minors

722 A covered entity may not engage in targeted advertising to any individual if the covered
723 entity has knowledge that the individual is a covered minor.

724 Section 11. Data Brokers

725 Each data broker shall place a clear, conspicuous, not misleading, and readily accessible
726 notice on the website or mobile application of the data broker (if the data broker maintains such a
727 website or mobile application) that:—

728 notifies individuals that the entity is a data broker;

729 includes a link to the data broker registry website; and

730 is reasonably accessible to and usable by individuals with disabilities.

731 Data broker registration. Not later than January 31 of each calendar year that follows a
732 calendar year during which a covered entity acted as a data broker, data brokers shall register
733 with the OCABR in accordance with this subsection.

734 In registering with the OCABR, a data broker shall do the following:—

735 Pay to the OCABR a registration fee of \$100;

736 Provide the OCABR with the following information:—

737 The legal name and primary physical, email, and internet addresses of the data broker;

738 A description of the categories of covered data the data broker processes and transfers;

739 (C) The contact information of the data broker, including a contact person, a telephone
740 number, an e-mail address, a website, and a physical mailing address; and

741 (D) A link to a website through which an individual may easily exercise the rights
742 provided under this subsection.

743 The OCABR shall establish and maintain on a website a searchable, publicly available,
744 central registry of third-party collecting entities that are registered with the OCABR under this
745 subsection that includes a listing of all registered data brokers and a search feature that allows
746 members of the public to identify individual data brokers and access to the registration
747 information provided under subsection (b).

748 Penalties. A data broker that fails to register or provide the notice as required under this
749 section shall be liable for:—

750 a civil penalty of \$100 for each day the data broker fails to register or provide notice as
751 required under this section, not to exceed a total of \$10,000 for any year; and

752 an amount equal to the registration fees for each year that the data broker failed to
753 register as required under this subsection.

754 Nothing in this subsection shall be construed as altering, limiting, or affecting any
755 enforcement authorities or remedies under this chapter.

756 Section 11. Civil rights protections

757 A covered entity or a service provider may not collect, process, or transfer covered data
758 or publicly available data in a manner that discriminates in or otherwise makes unavailable the
759 equal enjoyment of goods or services (i.e., has a disparate impact) on the basis of race, color,
760 religion, national origin, sex, sexual orientation, gender identity or disability.

761 This subsection shall not apply to:—

762 the collection, processing, or transfer of covered data for the purpose of:—

763 covered entity’s or a service provider’s self-testing to prevent or mitigate unlawful
764 discrimination; or

765 diversifying an applicant, participant, or customer pool; or

766 any private club or group not open to the public, as described in section 201(e) of the
767 Civil Rights Act of 1964, 42 U.S.C. section 2000a(e).

768 Whenever the Attorney General obtains information that a covered entity or service
769 provider may have collected, processed, or transferred covered data in violation of subsection
770 (a), the Attorney General shall initiate enforcement actions relating to such violation in
771 accordance with section (14) this chapter.

772 Not later than 3 years after the date of enactment of this chapter, and annually thereafter,
773 the Attorney General shall submit to the legislature a report that includes a summary of the
774 enforcement actions taken under this subsection.

775 Covered algorithm impact and evaluation. Notwithstanding any other provision of law,
776 not later than 2 years after the date of enactment of this chapter, and annually thereafter, a large
777 data holders that uses a covered algorithm in a manner that poses a consequential risk of harm to
778 an individual or group of individuals, and uses such covered algorithm solely or in part, to
779 collect, process, or transfer covered data or publicly available data shall conduct an impact
780 assessment of such algorithm in accordance with paragraph (1).

781 The impact assessment required under subsection (d) shall provide the following:—

782 A detailed description of the design process and methodologies of the covered algorithm;

783 A statement of the purpose and proposed uses of the covered algorithm;

784 A detailed description of the data used by the covered algorithm, including the specific
785 categories of data that will be processed as input and any data used to train the model that the
786 covered algorithm relies on, if applicable;

787 A description of the outputs produced by the covered algorithm as well as the outcomes
788 of their use;

789 An assessment of the necessity and proportionality of the covered algorithm in relation to
790 its stated purpose; and

791 A detailed description of steps the large data holder has taken or will take to mitigate
792 potential harms from the covered algorithm to an individual or group of individuals, including
793 related to:—

794 covered minors;

795 making or facilitating advertising for, or determining access to, or restrictions on the use
796 of housing, education, employment, healthcare, insurance, or credit opportunities;

797 determining access to, or restrictions on the use of, any place of public accommodation,
798 particularly as such harms relate to the protected characteristics of individuals, including race,
799 color, religion, national origin, sex, sexual orientation, gender identity or disability;

800 disparate impact on the basis of individuals' race, color, religion, national origin, sex,
801 sexual orientation, gender identity or disability status; or

802 disparate impact on the basis of individuals' political party registration status.

803 Notwithstanding any other provision of law, not later than 2 years after the date of
804 enactment of this chapter, a covered entity or service provider that knowingly develops a covered
805 algorithm that is designed, solely or in part, to collect, process, or transfer covered data in
806 furtherance of a consequential decision shall, prior to deploying the covered algorithm evaluate
807 the design, structure, and inputs of the covered algorithm, including any training data used to
808 develop the covered algorithm, to reduce the risk of the potential harms identified under the
809 previous paragraph.

810 In complying with paragraphs (1) and (2), a covered entity and a service provider may
811 focus the impact assessment or evaluation on any covered algorithm, or portions of a covered

812 algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms
813 identified under paragraph (2).

814 A covered entity and a service provider shall:—

815 submit the impact assessment or evaluation conducted under paragraph (1) or (2) to the
816 Attorney General not later than 30 days after completing an impact assessment or evaluation;

817 make such impact assessment and evaluation available to the legislature, upon request;

818 and

819 make a summary of such impact assessment and evaluation publicly available in a their
820 website or any other similar place that is easily accessible to individuals.

821 Covered entities and service providers may redact and segregate any trade secrets, as
822 defined in 18 U.S.C. section 1839, or other confidential or proprietary information from public
823 disclosure under this subsection.

824 The Attorney General may not use any information obtained solely and exclusively
825 through a covered entity or a service provider's disclosure of information to the Attorney
826 General in compliance with this section for any other purpose than enforcing this chapter;
827 provided, however, that it may be used for enforcing consent orders.

828 The previous subparagraph does not preclude the Attorney General from providing
829 information about a covered entity to the legislature in response to a subpoena.

830 Section 12. Miscellaneous

831 Not later than 18 months after the date of enactment of this chapter, the OCABR shall
832 establish or recognize one or more acceptable privacy protective, centralized mechanisms for
833 individuals to exercise the opt-out rights recognized in section 9.

834 Any such centralized opt-out mechanism shall:—

835 require covered entities or service providers acting on behalf of covered entities to inform
836 individuals about the centralized opt-out choice;

837 not be required to be the default setting, but may be the default setting provided that in all
838 cases the mechanism clearly represents the individual’s affirmative, freely given, and
839 unambiguous choice to opt out;

840 be consumer-friendly, clearly described, and easy-to-use by a reasonable individual;

841 be provided in any covered language in which the covered entity provides products or
842 services subject to the opt-out; and

843 be provided in a manner that is reasonably accessible to and usable by individuals with
844 disabilities.

845 A covered entity or service provider that is not a small business shall designate:—

846 1 or more qualified employees as privacy officers; and

847 1 or more qualified employees as data security officers.

848 An employee who is designated as a privacy officer or a data security officer pursuant to
849 subsection (c) shall, at a minimum:—

850 implement a data privacy program and data security program to safeguard the privacy
851 and security of covered data in compliance with the requirements of this chapter; and

852 facilitate the covered entity or service provider’s ongoing compliance with this chapter.

853 Each covered entity that is a large data holder shall conduct a privacy impact assessment
854 that weighs the benefits of the large data holder’s covered data collecting, processing, and
855 transfer practices against the potential adverse consequences of such practices, including
856 substantial privacy risks, to individual privacy.

857 The assessment shall be conducted not later than 1 year after the date of enactment of this
858 chapter or 1 year after the date on which a covered entity first meets the definition of large data
859 holder, whichever is earlier, and biennially thereafter.

860 A privacy impact assessment required under subsection (e) shall be:—

861 reasonable and appropriate in scope given:—

862 the nature of the covered data collected, processed, and transferred by the large data
863 holder;

864 the volume of the covered data collected, processed, and transferred by the large data
865 holder; and

866 the potential material risks posed to the privacy of individuals by the collecting,
867 processing, and transfer of covered data by the large data holder;

868 documented in written form and maintained by the large data holder unless rendered out
869 of date by a subsequent assessment conducted under subsection (e); and

870 approved by the privacy protection officer designated pursuant to subsection (c).

871 In assessing the privacy risks, including substantial privacy risks, the large data holder
872 must include reviews of the means by which technologies are used to secure covered data.

873 Section 13. Service providers.

874 A service provider:—

875 shall adhere to the instructions of a covered entity and only collect, process, and transfer
876 service provider data to the extent necessary and proportionate to provide a service requested by
877 the covered entity, as set out in the contract required by subsection (b), and this paragraph does
878 not require a service provider to collect, process, or transfer covered data if the service provider
879 would not otherwise do so;

880 may not collect, process, or transfer service provider data if the service provider has
881 actual knowledge that a covered entity violated this chapter with respect to such data;

882 shall assist a covered entity in responding to a request made by an individual under this
883 chapter, by either:—

884 providing appropriate technical and organizational measures, considering the nature of
885 the processing and the information reasonably available to the service provider, for the covered
886 entity to comply with such request for service provider data; or

887 fulfilling a request by a covered entity to execute an individual rights request that the
888 covered entity has determined should be complied with, by either:—

889 complying with the request pursuant to the covered entity's instructions; or

890 providing written verification to the covered entity that it does not hold covered data
891 related to the request, that complying with the request would be inconsistent with its legal
892 obligations, or that the request falls within an exception under this chapter;

893 may engage another service provider for purposes of processing service provider data on
894 behalf of a covered entity only after providing that covered entity with notice and pursuant to a
895 written contract that requires such other service provider to satisfy the obligations of the service
896 provider with respect to such service provider data, including that the other service provider be
897 treated as a service provider under this chapter;

898 shall, upon the reasonable request of the covered entity, make available to the covered
899 entity information necessary to demonstrate the compliance of the service provider with the
900 requirements of this chapter, which may include making available a report of an independent
901 assessment arranged by the service provider on terms agreed to by the service provider and the
902 covered entity, providing information necessary to enable the covered entity to conduct and
903 document a privacy impact assessment required by this chapter;

904 shall, at the covered entity's direction, delete or return all covered data to the covered
905 entity as requested at the end of the provision of services, unless retention of the covered data is
906 required by law;

907 shall develop, implement, and maintain reasonable administrative, technical, and physical
908 safeguards that are designed to protect the security and confidentiality of covered data the service
909 provider processes consistent with chapter 93H of the general laws; and

910 shall allow and cooperate with reasonable assessments by the covered entity or the
911 covered entity's designated assessor. Alternatively, the service provider may arrange for a

912 qualified and independent assessor to conduct an assessment of the service provider's policies
913 and technical and organizational measures in support of the obligations under this chapter using
914 an appropriate and accepted control standard or framework and assessment procedure for such
915 assessments. The service provider shall provide a report of such assessment to the covered entity
916 upon request.

917 A person or entity may only act as a service provider pursuant to a written contract
918 between the covered entity and the service provider, or a written contract between one service
919 provider and a second service provider as described under paragraph (4) of subsection (a), if the
920 contract:—

921 sets forth the data processing procedures of the service provider with respect to
922 collection, processing, or transfer performed on behalf of the covered entity or service provider;

923 clearly sets forth:—

924 instructions for collecting, processing, or transferring data;

925 the nature and purpose of collecting, processing, or transferring;

926 the type of data subject to collecting, processing, or transferring;

927 the duration of processing; and

928 the rights and obligations of both parties, including a method by which the service
929 provider shall notify the covered entity of material changes to its privacy practices;

930 does not relieve a covered entity or a service provider of any requirement or liability
931 imposed on such covered entity or service provider under this chapter; and

932 prohibits:—
933 collecting, processing, or transferring covered data in contravention to subsection (a); and
934 combining service provider data with covered data which the service provider receives
935 from or on behalf of another person or persons or collects from the interaction of the service
936 provider with an individual, provided that such combining is not necessary to effectuate a
937 purpose described in paragraphs (1) through (15) of section 2(a) and is otherwise permitted under
938 the contract required by this subsection.

939 Each service provider shall retain copies of previous contracts entered into in compliance
940 with this subsection with each covered entity to which it provides requested products or services.

941 The classification of a person or entity as a covered entity or as a service provider and the
942 relationship between covered entities and service providers are regulated by the following
943 provisions:—

944 Determining whether a person is acting as a covered entity or service provider with
945 respect to a specific processing of covered data is a fact-based determination that depends upon
946 the context in which such data is processed.

947 A person or entity that is not limited in its processing of covered data pursuant to the
948 instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and
949 not a service provider with respect to a specific processing of covered data. A service provider
950 that continues to adhere to the instructions of a covered entity with respect to a specific
951 processing of covered data remains a service provider. If a service provider begins, alone or

952 jointly with others, determining the purposes and means of the processing of covered data, it is a
953 covered entity and not a service provider with respect to the processing of such data.

954 A covered entity that transfers covered data to a service provider or a service provider
955 that transfers covered data to a covered entity or another service provider, in compliance with the
956 requirements of this chapter, is not liable for a violation of this chapter by the service provider or
957 covered entity to whom such covered data was transferred, if at the time of transferring such
958 covered data, the covered entity or service provider did not have actual knowledge that the
959 service provider or covered entity would violate this chapter.

960 A covered entity or service provider that receives covered data in compliance with the
961 requirements of this chapter is not in violation of this chapter as a result of a violation by a
962 covered entity or service provider from which such data was received.

963 A third party:—

964 shall not process third party data for a processing purpose other than the processing
965 purpose for which—

966 the individual gave affirmative express consent or to effect a purpose enumerated in
967 paragraph (2), (3), or (5) of subsection (a) of section 2 in the case of sensitive covered data; or

968 the covered entity made a disclosure pursuant to their privacy policy and in the case of
969 data that is not sensitive data;

970 may reasonably rely on representations made by the covered entity that transferred the
971 third-party data if the third party conducts reasonable due diligence on the representations of the
972 covered entity and finds those representations to be credible.

973 Solely for the purposes of this section, the requirements for service providers to contract
974 with, assist, and follow the instructions of covered entities shall be read to include requirements
975 to contract with, assist, and follow the instructions of a government entity if the service provider
976 is providing a service to a government entity.

977 Section 14. Enforcement. Private Right of Action and Attorney General enforcement.

978 A violation of this chapter or a regulation promulgated under this chapter constitutes an
979 injury to that individual.

980 Private right of action. Any individual alleging a violation of this chapter by a covered
981 entity that is not a small business may bring a civil action in the superior court or any court of
982 competent jurisdiction.

983 An individual protected by this chapter may not be required, as a condition of service or
984 otherwise, to file an administrative complaint with the commission or to accept mandatory
985 arbitration of a claim under this chapter.

986 The civil action shall be directed to the covered entity, data processor, and the third-
987 parties alleged to have committed the violation.

988 In a civil action in which the plaintiff prevails, the court may award:—

989 liquidated damages of not less than 0.15% of the annual global revenue of the covered
990 entity or \$15,000 per violation, whichever is greater;

991 punitive damages; and

992 any other relief, including but not limited to an injunction, that the court deems to be
993 appropriate.

994 In addition to any relief awarded pursuant to the previous paragraph, the court shall
995 award reasonable attorney's fees and costs to any prevailing plaintiff.

996 The attorney general may bring an action pursuant to section 4 of chapter 93A against a
997 covered entity, service provider, third party or data broker to remedy violations of this chapter
998 and for other relief that may be appropriate.

999 If the court finds that the defendant has employed any method, chapter, or practice which
1000 they knew or should have known to be in violation of this chapter, the court may require such
1001 person to pay to the commonwealth a civil penalty of:—

1002 not less than 0.15% of the annual global revenue or \$15,000, whichever is greater, per
1003 violation; and

1004 not more than 4% of the annual global revenue of the covered entity, data processor, or
1005 third-party or \$20,000,000, whichever is greater, per action if such action includes multiple
1006 violations to multiple individuals;

1007 All money awards shall be paid to the commonwealth. The commonwealth shall identify
1008 the individuals affected by the violation and earmark such money awards, penalties, or
1009 assessments collected for purposes of paying for the damages they suffered as a consequence of
1010 the violation.

1011 When calculating awards and civil penalties in all the actions in this section, the court
1012 shall consider:—

1013 the number of affected individuals;

1014 the severity of the violation or noncompliance;

1015 the risks caused by the violation or noncompliance;

1016 whether the violation or noncompliance was part of a pattern of noncompliance and

1017 violations and not an isolated instance;

1018 whether the violation or noncompliance was willful and not the result of error;

1019 the precautions taken by the defendant to prevent a violation;

1020 the number of administrative actions, lawsuits, settlements, and consent-decrees under

1021 this chapter involving the defendant;

1022 the number of administrative actions, lawsuits, settlements, and consent-decrees

1023 involving the defendant in other states and at the federal level in issues involving information

1024 privacy; and

1025 the international record of the defendant when it comes to information privacy issues.

1026 It is a violation of this chapter for a covered entity or anyone else acting on behalf of a

1027 covered entity to retaliate against an individual who makes a good-faith complaint that there has

1028 been a failure to comply with any part of this chapter.

1029 An injured individual by a violation of the previous paragraph may bring a civil action

1030 for monetary damages and injunctive relief in any court of competent jurisdiction.

1031 Section 15. Enforcement - Miscellaneous

1032 Any provision of a contract or agreement of any kind, including a covered entity’s terms
1033 of service or a privacy policy, including the short-form privacy notice required under section 3
1034 that purports to waive or limit in any way an individual’s rights under this chapter, including but
1035 not limited to any right to a remedy or means of enforcement shall be deemed contrary to public
1036 policy and shall be void and unenforceable.

1037 No covered entity that is a provider of an interactive computer service, as defined in 47
1038 U.S.C. section 230, shall be treated as the publisher or speaker of any personal information
1039 provided by another information content provider, as defined in 47 U.S.C. section 230 and
1040 allowing posting of information by a user without other action by the interactive computer
1041 service shall not be deemed processing of the personal information by the interactive computer
1042 service.

1043 No private or government action brought pursuant to this chapter shall preclude any other
1044 action under this chapter.

1045 Section 16. Transparency

1046 Covered entities that receive any form of a legal request for disclosure of personal
1047 information pursuant to this chapter shall:—

1048 provide the Attorney General and the general public a bi-monthly report containing the
1049 following aggregate information related to legal requests received by the covered entity, their
1050 affiliated data processors, and any third parties they contracted with:—

1051 The total number of legal requests, disaggregated by type of requests such as warrants,
1052 court orders, and subpoenas;

1053 The number of legal requests that resulted in the covered entity disclosing personal
1054 information;

1055 The number of legal requests that did not result in the covered entity disclosing personal
1056 information, including the reasons why the information was not disclosed;

1057 The type of personal information sought in the legal requests received by the covered
1058 entity;

1059 The total number of legal requests seeking the disclosure of location or biometric
1060 information;

1061 The number of legal requests that resulted in the covered entity disclosing location or
1062 biometric information;

1063 The number of legal requests that did not result in the covered entity disclosing location
1064 or biometric information, including the reasons for such no disclosure; and

1065 The nature of the proceedings from which the requests were ordered and whether it was a
1066 government entity or a private person seeking the legal request;

1067 take all reasonable measures and engage in all legal actions available to ensure that the
1068 legal request is valid under applicable laws and statutes; and

1069 require their affiliate data processors and third parties they contracted with to have
1070 similar practices and standards.

1071 Section 17. Non-applicability

1072 This chapter shall not apply to:—

1073 personal information captured from a patient by a health care provider or health care
1074 facility or biometric information collected, processed, used, or stored exclusively for medical
1075 education or research, public health or epidemiological purposes, health care treatment,
1076 insurance, payment, or operations under the federal Health Insurance Portability and
1077 Accountability chapter of 1996, or to X-ray, roentgen process, computed tomography, MRI, PET
1078 scan, mammography, or other image or film of the human anatomy used exclusively to diagnose,
1079 prognose, or treat an illness or other medical condition or to further validate scientific testing or
1080 screening;

1081 individuals sharing their personal contact information such as email addresses with other
1082 individuals in the workplace, or other social, political, or similar settings where the purpose of
1083 the information is to facilitate communication among such individuals, provided that this chapter
1084 shall cover any processing of such contact information beyond interpersonal communication; or
1085 covered entities' publication of entity-based member or employee contact information
1086 where such publication is intended to allow members of the public to contact such member or
1087 employee in the ordinary course of the entity's operations.

1088 Section 18. Relationship with other laws

1089 Nothing in this chapter shall diminish any individual's rights or obligations under the
1090 Massachusetts Fair Information Practices chapter and its regulations.

1091 Section 19. Implementation

1092 The Attorney General shall:—

1093 adopt, amend, or repeal regulations for the implementation, administration, and
1094 enforcement of this chapter;

1095 gather facts and information applicable to the Attorney General’s obligation to enforce
1096 this chapter and ensure its compliance;

1097 conduct investigations for possible violations of this chapter;

1098 refer cases for criminal prosecution to the appropriate federal, state, or local authorities;
1099 and

1100 maintain an official internet website outlining the provisions of this Act.

1101 Section 20. Severability

1102 Should any provision of this chapter or part hereof be held under any circumstances in
1103 any jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect
1104 the validity or enforceability of any other provision of this or other parts of this chapter.

1105

1106 SECTION 2. Chapter 149 of the General Laws, as appearing in the 2018 Official Edition,
1107 is hereby amended by inserting after section 203 the following section:—

1108 Section 204. Workplace Surveillance

1109 For the purposes of this section, the following words shall have the following meanings
1110 unless the context clearly requires otherwise:—

1111 “Information” also referred to as “employee information,” or “employee data”,
1112 information that identifies, relates to, describes, is reasonably capable of being associated with,
1113 or could reasonably be linked, directly or indirectly, with a particular employee, regardless of
1114 how the information is collected, inferred, or obtained.

1115 “Electronic monitoring”, the collection of information concerning employee activities,
1116 communications, actions, biometrics, or behaviors by electronic means.

1117 “Employment-related decision”, any decision made by the employer that affects wages,
1118 benefits, hours, work schedule, performance evaluation, hiring, discipline, promotion,
1119 termination, job content, productivity requirements, workplace health and safety, or any other
1120 terms and conditions of employment.

1121 “Vendor”, a business engaged in a contract with an employer to provide services,
1122 software, or technology that collects, stores, analyzes, or interprets employee information.

1123 “Facial recognition technology” shall have the meaning established in section 220 of
1124 chapter 6 of the General Laws, as amended by Chapter 253 of the Acts of 2020.

1125 An employer, or vendor acting on behalf of an employer, shall not electronically monitor
1126 an employee unless:—

1127 the electronic monitoring only purpose is to:—

1128 enable tasks that are necessary to accomplish essential job functions;

1129 monitor production processes or quality;

1130 comply with employment, labor, or other relevant laws;

1131 protect the safety and security of employees; or
1132 carry on other purposes as determined by the department of labor standards; and
1133 the specific form of electronic monitoring is:—
1134 necessary to accomplish the allowable purpose;
1135 the least invasive means that could reasonably be used to accomplish the allowable
1136 purpose;
1137 limited to the smallest number of employees; and
1138 collecting the least amount of information necessary to accomplish the purpose
1139 mentioned in (1).
1140 Notwithstanding subsection (b), the following practices shall be prohibited:—
1141 use of electronic monitoring that either directly or indirectly harms an employee’s
1142 physical health, mental health, personal safety or wellbeing;
1143 monitoring of employees who are off-duty and not performing work-related tasks;
1144 audio-visual monitoring of bathrooms or other similarly private areas including locker
1145 rooms and changing areas;
1146 audio-visual monitoring of break rooms, lounges, and other social spaces, except to
1147 investigate specific illegal activity;
1148 use of facial recognition technology other than for the purpose of verifying the identity of
1149 an employee for security purposes; and

1150 any other forms of electronic monitoring such as may be prohibited by the department of
1151 labor standards.

1152 Employers shall not require employees to install applications on personal or mobile
1153 devices that collect employee information or require employees to wear data-collecting devices,
1154 including those that are incorporated into items of clothing or personal accessories, unless the
1155 electronic monitoring is necessary to accomplish essential job functions and is narrowly limited
1156 to only the activities and times necessary to accomplish essential job functions.

1157 Information resulting from electronic monitoring shall be accessed only by authorized
1158 agents and used only for the purpose and duration for which notice was given in accordance with
1159 subsection (f).

1160 Employers shall provide employees with notice that electronic monitoring will occur
1161 prior to conducting each specific form of electronic monitoring. The notice must, at a minimum,
1162 include:—

1163 a description of:—

1164 the purpose that the specific form of electronic monitoring is intended to accomplish, as
1165 specified in subsection (b);

1166 the specific activities, locations, communications, and job roles that will be electronically
1167 monitored;

1168 the technologies used to conduct the specific form of electronic monitoring;

1169 the vendors or other third parties that information collected through electronic monitoring
1170 will be disclosed or transferred to, including the name of the vendor and the purpose for the data
1171 transfer;

1172 the organizational positions that are authorized to access the information collected
1173 through the specific form of electronic monitoring, and under what conditions; and

1174 the dates, times, and frequency that electronic monitoring will occur;

1175 the names of any vendors conducting electronic monitoring on the employer's behalf; and

1176 an explanation of:—

1177 the reasons why the specific form of electronic monitoring is necessary to accomplish the
1178 purpose; and

1179 how the specific monitoring practice is the least invasive means available to accomplish
1180 the allowable monitoring purpose.

1181 The notice mentioned in (f) shall be clear and conspicuous and provide the employee
1182 with actual notice of electronic monitoring activities.

1183 A notice that provides electronic monitoring "may" take place or that the employer
1184 "reserves the right" to monitor shall not suffice.

1185 An employer who engages in random or periodic electronic monitoring of employees will
1186 inform the affected employees of the specific events which are being monitored at the time the
1187 monitoring takes place with a notice that shall be clear and conspicuous.

1188 Notwithstanding the previous paragraph, notice of random or periodic electronic
1189 monitoring may be given after electronic monitoring has occurred only if necessary to preserve
1190 the integrity of an investigation of wrongdoing or protect the immediate safety of employees,
1191 customers, or the public.

1192 Employers shall provide a copy of the above notice disclosure to the department of labor
1193 standards.

1194 An employer shall only use employee information collected through electronic
1195 monitoring to accomplish its purpose, unless the information documents illegal activity.

1196 When making a hiring or employment-related decision using information collected
1197 through electronic monitoring, an employer shall:—

1198 not make the decision based solely on such information;

1199 give the affected employee access to the data and provide an opportunity to correct or
1200 explain it;

1201 corroborate such information by other means, such as independent documentation by
1202 supervisors or managers, or by consultation with other employees; and

1203 document and communicate to affected employees the basis for the corroboration prior to
1204 the decision going into effect.

1205 Subsection (k) shall not apply to those cases when electronic monitoring data provides
1206 evidence of illegal activity.

1207

1208

SECTION 3. Effective date.

1209

The provisions of this Act shall take effect 12 months after this Act is enacted.

1210

The enforcement of chapter 93L shall be delayed until 6 months after the effective date.

1211

1212