

HOUSE No. 136

The Commonwealth of Massachusetts

PRESENTED BY:

David M. Rogers and Andres X. Vargas

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 relative to data privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>David M. Rogers</i>	<i>24th Middlesex</i>	<i>2/19/2021</i>
<i>Andres X. Vargas</i>	<i>3rd Essex</i>	<i>2/21/2021</i>
<i>Patrick Joseph Kearney</i>	<i>4th Plymouth</i>	<i>2/22/2021</i>
<i>Kate Lipper-Garabedian</i>	<i>32nd Middlesex</i>	<i>2/26/2021</i>
<i>David Henry Argosky LeBoeuf</i>	<i>17th Worcester</i>	<i>2/26/2021</i>
<i>Lindsay N. Sabadosa</i>	<i>1st Hampshire</i>	<i>2/26/2021</i>
<i>Dylan A. Fernandes</i>	<i>Barnstable, Dukes and Nantucket</i>	<i>3/8/2021</i>
<i>Bradley H. Jones, Jr.</i>	<i>20th Middlesex</i>	<i>3/9/2021</i>
<i>Elizabeth A. Malia</i>	<i>11th Suffolk</i>	<i>3/15/2021</i>
<i>David Allen Robertson</i>	<i>19th Middlesex</i>	<i>3/16/2021</i>
<i>Jessica Ann Giannino</i>	<i>16th Suffolk</i>	<i>11/16/2021</i>

HOUSE No. 136

By Messrs. Rogers of Cambridge and Vargas of Haverhill, a petition (accompanied by bill, House, No. 136) of David M. Rogers, Andres X. Vargas and others relative to data privacy. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Second General Court
(2021-2022)**

An Act relative to data privacy.

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 are hereby amended by inserting after chapter 93K the
2 following chapter:-

3 CHAPTER 93L. Data Accountability and Transparency Agency.

4 Section 1. Definitions.

5 For purpose of this chapter, the following words and terms shall have the following
6 meanings:

7 “Affiliate”, means any person that controls, is controlled by, or is under common control
8 with another person.

9 “Agency”, means the Massachusetts Data Accountability and Transparency Agency
10 established in section 5.

11 “Anonymized Data”, means information that has been proven to not identify, relate to,
12 describe, reference, be capable of being associated with, or be linked or reasonably linkable to a
13 particular individual or device.

14 “Automated Decision System”, means a computational process, including one derived
15 from machine learning, statistics, or other data processing or artificial intelligence techniques,
16 that makes a decision, or facilitates human decision-making.

17 “Automated decision system impact evaluation”, means a study conducted after
18 deployment of an automated decision system that includes, at a minimum—(a) an evaluation of
19 an automated decision system’s accuracy, bias on the basis of protected class, and impact on
20 privacy on individuals or groups of individuals; (b) an evaluation of the effectiveness of
21 measures taken to minimize risks as outlined in any prior automated decision system risk
22 assessments; and (c) recommended measures to further minimize risks to accuracy, bias on the
23 basis of protected class, and privacy on individuals or groups of individuals.

24 “Automated decision system risk assessment”, means a study evaluating an automated
25 decision system and the automated decision system’s development process, including the design
26 and training data of the automated decision system, for potential risks to accuracy, bias,
27 discrimination, and privacy on individuals or groups of individuals that includes, at a
28 minimum—(a) a detailed description of the automated decision system, including—(i) its design
29 and methodologies; (ii) training data characteristics; (iii) data; and (iv) purpose; (b) an
30 assessment of the automated decision system governance in light of its purpose, potential
31 unintended consequences, and taking into account relevant factors, including—(i) the duration
32 and methods for which personal data and the results of the automated decision system are stored;

33 (ii) what information about the automated decision system (including inputs, features, and
34 results) is available to individuals; and (iii) the recipients of the results of the automated decision
35 system; (c) an assessment of the risks posed by the automated decision system—(i) poses to
36 individuals or groups of individuals of privacy harm; and (ii) may result in or contribute to in
37 accurate, biased, or discriminatory decisions impacting individuals or groups of individuals; (D)
38 the measures a data aggregator will employ to minimize the risks described in subparagraph (C),
39 including technological and physical safeguards.

40 “Collect”, (a) means buying, renting, gathering, obtaining, receiving, or accessing any
41 personal data by any means; and (b) includes—(i) receiving personal data from an individual or
42 device; and (ii) creating, deriving, or inferring personal data by observing the behavior of an
43 individual.

44 “Commissioner,” means the Commissioner of the Massachusetts Data Accountability and
45 Transparency Agency.

46 “Covered individual”, means an applicant, current or former employee, contractor,
47 subcontractor, grantee, or agent of a data aggregator or service provider.

48 “Data Aggregator”, means (a) any person that collects, uses, or shares an amount of
49 personal data that is not de minimis; and (b) does not include an individual who collects, uses, or
50 shares personal data solely for personal reasons.

51 “Device”, means any physical object that— (a) is capable of connecting to the internet or
52 other communication network; or (b) has computer processing capabilities that can collect, send,
53 receive, or store data.

54 “Electronic data”, means any information that is in an electronic or digital format or any
55 electronic or digital reference that contains information about an individual or device.

56 “Facial recognition technology”, means an automated or semiautomated process that
57 assists in identifying or verifying an individual based on the characteristics of the face of an
58 individual.

59 “Individual”, means a natural person.

60 “Intentional interaction”, means an interaction in which an individual engages in 1 or
61 more actions to demonstrate that the individual intends to interact with a data aggregator.

62 “Journalism”, means the gathering, preparing, collecting, photographing, recording,
63 writing, editing, reporting, or publishing of news or information that concerns local, national, or
64 international events or other matters of public interest for dissemination to the public; and
65 includes the collection or use of personal data about a public individual or official, or that
66 otherwise concerns matters of public interest, for dissemination to the public.

67 “Person”, means an individual, a local, State, or Federal governmental entity, a
68 partnership, a company, a corporation, an association (incorporated or unincorporated), a trust,
69 an estate, a cooperative organization, another entity, or any other organization or group of such
70 entities acting in concert.

71 “Personal data”, means electronic data that, alone or in combination with other data—(A)
72 could be linked or reasonably linkable to an individual, household, or device; or (B) could be
73 used to determine that an individual or household is part of a protected class.

74 “Privacy harm” means an adverse consequence, or a potential adverse consequence, to
75 an individual, a group of individuals, or society caused, or potentially caused, in whole or in part,
76 by the collection, use, or sharing of personal data, including—(a) direct or indirect financial loss
77 or economic harm, including financial loss or economic harm arising from fraudulent activities
78 or data security breaches; (b) physical harm, harassment, or a threat to an individual or property;
79 (c) psychological harm, including anxiety, embarrassment, fear, other trauma, stigmatization,
80 reputational harm, or the revealing or exposing of an individual, or a characteristic of an
81 individual, in an unexpected way; (d) an adverse outcome or decision, including relating to the
82 eligibility of an individual for the rights, benefits, or privileges in credit and insurance (including
83 the denial of an application or obtaining less favorable terms), housing, education, professional
84 certification, employment (including hiring, firing, promotion, demotion, and compensation), or
85 the provision of health care and related services; (e) discrimination or the otherwise unfair or
86 unethical differential treatment with respect to an individual, including in a manner that is
87 prohibited under Section 9 of this chapter; (f) the interference with, or the surveillance of,
88 activities that are protected by the First Amendment to the Constitution of the United States; (g)
89 the chilling of free expression or action of an individual, or society generally, due to perceived or
90 actual pervasive and excessive collection, use, or sharing of personal data; (h) the impairment of
91 the autonomy of an individual or society generally; and (i) any harm fairly traceable to an
92 invasion of privacy tort; and (j) any other adverse consequence, or potential adverse
93 consequence, consistent with the provisions of this Act, as determined by the Director.

94 “Protected class”, means the actual or perceived race, color, ethnicity, national origin,
95 religion, sex, gender, gender identity, sexual orientation, familial status, biometric information,
96 lawful source of income, or disability of an individual or a group of individuals.

97 “Public accommodation” means any type of business considered a place of public
98 accommodation pursuant to section 201(b) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(b))
99 or section 301(7) of the Americans with Disabilities Act of 1990 (42 U.S.C. 12181(7)) or a
100 business that offers goods or services through the internet to the general public.

101 “Service provider”, means a data aggregator that collects, uses, or shares personal data
102 only on behalf of another data aggregator in order to carry out a permissible purpose.

103 “Share”, means disseminating, making available, transferring, or otherwise
104 communicating orally, in writing, or by electronic or other means, personal data, except for as
105 required under section 9 of this chapter.

106 “Use”, means to perform an operation or a set of operations on personal data, either
107 manually or by automated means, after the collection of the data, including—(a) the analysis,
108 organization, storage, retention, or maintenance of the data; and (b) the derivation or inference of
109 information from the personal data.

110 “Verifiable request”, means a request that a data aggregator can reasonably verify is
111 made—(a) by an individual; (b) by an individual on behalf of the individual’s minor child; or (c)
112 by a person registered with the Secretary of State authorized by the individual to act on the
113 individual’s behalf.

114 Section 2. Massachusetts Data Accountability and Transparency Agency.

115 (a) There shall be a Massachusetts Data Accountability and Transparency Agency which
116 shall consist of one commissioner who shall exercise supervision and control over the agency,
117 whom shall be appointed by a majority vote of the treasurer and receiver-general, the governor,

118 and the attorney general and shall have a background in technology; protection of personal data;
119 civil rights and liberties; law; social sciences; and business.

120 (b) The commissioner shall serve in that capacity for a term of five years and until a
121 successor shall be appointed. The commissioner shall be eligible for reappointment; provided,
122 however that no commissioner shall serve more than 10 years. An individual appointed to fill the
123 vacancy of commissioner shall be appointed in a like manner.

124 (c) The commissioner shall be a resident of the commonwealth within 90 days of
125 appointment and, while serving as commissioner, shall not: (i) hold, or be a candidate for,
126 federal, state or local elected office; (ii) hold an appointed office in a federal, state or local
127 government; or (iii) serve as an official in a political party. The commissioner shall receive a
128 salary equal to the salary of the secretary of administration and finance under section 4 of chapter
129 7. The commissioner shall devote their full time and attention to the duties of their office and
130 shall hold no other employment.

131 (d) The treasurer and receiver-general, the governor, and the attorney general may
132 remove the commissioner, by a majority vote, if the commissioner: (i) is guilty of malfeasance in
133 office; (ii) substantially neglects the duties of a commissioner; (iii) is unable to discharge the
134 powers and duties of the office; (iv) commits gross misconduct; or (v) is convicted of a felony.
135 Before removal, the commissioner shall be provided with a written statement of the reason for
136 removal and shall have an opportunity to be heard.

137 (e) The commissioner, through the agency, shall have all the powers necessary or
138 convenient to carry out and effectuate its purposes including, but not limited to, the power to: (i)
139 appoint officers, hire employees and make such divisions or other offices among employees of

140 the agency; (ii) establish and amend a plan of organization that it considers expedient; (iii)
141 execute all instruments necessary or convenient for accomplishing the purposes of this chapter;
142 (iv) enter into agreements or other transactions with a person, including, but not limited to, a
143 public entity or other governmental instrumentality or authority in connection with its powers
144 and duties under this chapter; (v) appear on its own behalf before boards, commissions,
145 departments or other agencies of municipal, state or federal government; (vi) apply for and
146 accept subventions, grants, loans, advances and contributions of money, property, labor or other
147 things of value from any source, to be held, used and applied for its purposes; (vii) provide and
148 pay for advisory services and technical assistance as may be necessary in its judgment to carry
149 out this chapter and fix the compensation of persons providing such services or assistance; (viii)
150 prepare, publish and distribute, with or without charge as the commissioner may determine, such
151 studies, reports, bulletins and other materials as the commissioner considers appropriate; (ix)
152 gather facts and information applicable to the agency's obligations; (x) conduct investigations
153 into covered entities, including data aggregators and service providers; (xi) impose fees and
154 fines, as authorized by this chapter and penalties and sanctions for a violation of this chapter or
155 any regulations promulgated by the agency; (xii) collect fees under this chapter; (xiii) conduct
156 adjudicatory proceedings and promulgate regulations in accordance with chapter 30A and may
157 adopt regulations and establish procedures that include electronic communications, by which a
158 request to receive notice shall be made and the method by which timely notice may be given;
159 (xiv) refer cases for criminal prosecution to the appropriate federal, state or local authorities; (xv)
160 maintain an official internet website for the agency; (xvi) monitor any federal activity regarding
161 data privacy; (xvii) delegate to any employee, representative, or agent any powers vested in the
162 agency by law; (xviii) adopt and use a seal; (xix) use and expend funds; (xx) implement this

163 chapter through orders, guidance documents, interpretations, statements of policy, examinations,
164 investigations, joint investigations, and enforcement actions; (xxi) monitor risks to individuals or
165 groups of individuals in collection, use, and sharing of personal data and report risks to the
166 public; and (xxii) perform such other functions as may be authorized or required by law.

167 (f) The commissioner shall file an annual report with the secretary of the executive office
168 of administration and finance, the clerks of the senate and the house of representatives, and the
169 senate and house committees on ways and means: (i) listing the number of employees of the
170 agency, the salaries and titles of each employee, the source of funding for the salaries of said
171 employees and the projected date when federal funds for such positions are expected to
172 terminate; (ii) listing and describing grant programs of the department funded by the federal
173 government, including the amount of funding by grant; (iii) listing and describing other programs
174 of the agency; and (iv) any other amounts to be spent by category and grantee. Such reports shall
175 be filed annually on or before December thirty-first and shall refer to activities planned for the
176 subsequent calendar year. The commissioner shall also file with said committees an annual
177 report detailing all expenditures in the agency by the division, identified by categories of projects
178 and grantees under each category, together with all available documentation resulting from such
179 expenditures. Such reports shall be filed on or before March first of each year and shall refer to
180 activities in the preceding calendar year.

181 (g) The commissioner shall be sworn to the faithful performance of their official duties.
182 The commissioner shall not own, or be in the employ of, or own any stock in any data aggregator
183 or data service provider nor shall they be in any way directly or indirectly pecuniarily interested
184 in or connected with any such company or in the employ or connected with any person financing
185 any such company. The commissioner shall not personally or through any partner or agent render

186 any professional service or make or perform any business contract with or for any data
187 aggregator or data service provider, nor shall the commissioner directly or indirectly receive any
188 commission, bonus, discount, present, or reward from any such company.

189 (h) The commissioner shall appoint an executive director. The executive director shall
190 serve at the pleasure of the commissioner and shall receive $\frac{3}{4}$ the salary of the commissioner, and
191 shall devote full time and attention to the duties of the office and shall hold no other employment
192 during their period of service. The executive director shall be a person with skill and experience
193 in management, shall be the executive and administrative head of the agency and shall be
194 responsible for administering and enforcing the law relative to the agency and to each
195 administrative unit thereof. With the consent of the commissioner, the executive director shall
196 appoint and employ a chief financial and accounting officer and may, employ other employees,
197 consultants, agents and advisors, including legal counsel. The executive director shall attend all
198 meetings of the agency. In the case of an absence or vacancy in the office of the executive
199 director or in the case of disability, the commissioner may appoint an acting executive director to
200 serve as the executive director until the commissioner appoints another executive director. The
201 acting executive director shall have all of the powers and duties of the executive director and
202 shall have similar qualifications as the executive director.

203 (i) The commissioner shall appoint a secretary. The secretary shall keep a record of the
204 proceedings of the agency and shall be the custodian and keeper of the records of all books,
205 documents and papers filed by the agency and of its minutes book. The secretary shall cause
206 copies to be made of all minutes and other records and documents of the agency and shall certify
207 that such copies are true copies and all persons dealing with the agency may rely upon such
208 certification.

209 (j) The chief financial and accounting officer of the agency shall be in charge of its funds,
210 books of account and accounting records. No funds shall be transferred by the agency without
211 the approval of the commissioner and the signatures of the chief financial and accounting officer
212 and the secretary of the agency.

213 (k) Chapters 268A and 268B shall apply to the commissioner and to employees of the
214 agency; provided, however, that the commissioner shall establish a code of ethics for all
215 members and employees that shall be more restrictive than said chapters 268A and 268B. A copy
216 of the code shall be filed with the state ethics commission. The code shall include provisions
217 reasonably necessary to carry out the purposes of this section and any other laws subject to the
218 jurisdiction of the agency including, but not limited to: (i) prohibiting the receipt of gifts by the
219 commissioner and employees from any data aggregator, service provider, close associate,
220 affiliate or other person or entity subject to the jurisdiction of the agency; (ii) prohibiting the
221 participation by the commissioner and employees in a particular matter as defined in section 1 of
222 said chapter 268A that affects the financial interest of a relative within the third degree of
223 consanguinity or a person with whom such commissioner or employee has a significant
224 relationship as defined in the code; and (iii) providing for recusal of the commissioner in an
225 agency decision due to a potential conflict of interest.

226 (l) The Massachusetts Data Accountability and Transparency Agency shall be a
227 commission for the purposes of section 3 of chapter 12.

228 (m) The agency shall, for the purposes of compliance with state finance law, operate as a
229 state agency as defined in section 1 of chapter 29 and shall be subject to the laws applicable to
230 agencies under the control of the governor, provided, however, that the comptroller may identify

231 any additional instructions or actions necessary for the department to manage fiscal operations in
232 the state accounting system and meet statewide and other governmental accounting and audit
233 standards. The agency shall properly classify the agency's operating and capital expenditures,
234 and shall not include any salaries of employees in the agency's capital expenditures. Unless
235 otherwise exempted by law or the applicable central service agency, the agency shall participate
236 in any other available commonwealth central services including, but not limited to, the state
237 payroll system pursuant to section 31 of said chapter 29, and may purchase other goods and
238 services provided by state agencies in accordance with comptroller provisions. The comptroller
239 may chargeback the agency for the transition and ongoing costs for participation in the state
240 accounting and payroll systems and may retain and expend such costs without further
241 appropriation for the purposes of this section. The agency shall be subject to section 5D and
242 subsection (f) of section 6B of said chapter 29.

243 (n) The governor, attorney general, and treasurer and receiver-general shall each appoint
244 one governor respectfully to the board of governors, who shall oversee and manage the funds of
245 the Data Relief Fund; provided, that the three governors shall serve a term of five years and
246 whose replacement shall be appointed in a like manner. The governors shall have a background
247 with similar experience as the commissioner or in finance.

248 (o) The board of governors shall have the power to create rules, procedures, and
249 management of all funds established in section 7(c) of this chapter.

250 Section 3. Agency's Purpose, Objectives, and Functions.

251 (a) The Agency shall seek to protect individuals' privacy and enforce this chapter's
252 limitations on the collection, use, and sharing of personal data and other federal and state privacy
253 law, and is authorized to exercise its authorities under this chapter for such purposes.

254 (b) The agency is authorized to exercise its authorities under this chapter for the
255 following purposes: (i) protect individuals from violation of this chapter or other federal or state
256 privacy laws or unfair, deceptive, abusive, or discriminatory data practices. (ii) ensure that
257 federal and state privacy law is enforced consistently and in order to protect individuals and
258 ensure fair competition; and (iii) the agency shall work with other agencies to execute their
259 authority under this chapter.

260 (c) The agency shall function to: (i) provide leadership and coordination to efforts of all
261 state departments and agencies to enforce all laws, executive orders, relations and policy which
262 involve privacy of data protection; (ii) maximize effort, promote efficiency, and eliminate
263 conflict, competition, duplication, and inconsistency among the operations, functions, and
264 jurisdictions of federal and state departments and agencies responsible for privacy or data
265 protection, data protection rights and standards, and fair information practices and principals;
266 (iii) provide active leadership, guidance, education and appropriate assistance to private sector
267 businesses, and organizations, groups, institutions, and individuals regarding privacy, data
268 protection rights and standards, and fair information practices and principals; (iv) require and
269 oversee ex-ante impact assessments and ex-post outcomes audits of high-risk data practices by
270 data aggregators or covered entities to advance fair and just data practices; (v) examining the
271 social, ethical, economic, and civil rights impacts of high-risk data practices and propose
272 remedies; (vi) ensure that data privacy practices are fair, just, and nondiscriminatory, and comply
273 with fair information practices; (vii) collect, research, and respond to complaints; (viii) develop

274 model privacy, data protection, and fair information practices, standards, guidelines, policies,
275 and routine uses for use by the private sector; (ix) issue rules, orders, and guidance implementing
276 this act; and (x) enforce other privacy statutes and rules as authorized by federal and state law.

277 (d) The agency and its employees are authorized to exercise its authorities under this
278 chapter to administer, enforce, and otherwise implement the provisions of this chapter.

279 (e) The agency may require reports and conduct examinations on a periodic basis of data
280 aggregators, who have annual gross revenues that exceed \$25,000,000 or who annually collects,
281 uses, or shares, alone or in combination, the personal data of 50,000 or more individuals,
282 households, or devices, for purposes of: (i) assessing compliance with requirements of this
283 chapter or other federal and state laws; (ii) obtaining information of activities subject to such
284 laws and the associated compliance systems or procedures for such entities; (iii) detecting and
285 assessing associated risks to individuals and groups; and (iv) requiring and overseeing ex-ante
286 impact assessments and ex-post outcome audits of automated decision systems to advance fair
287 and just data practices.

288 (f)(i)The agency may take any action authorized under this chapter to prevent a data
289 aggregator or service provider from committing or engaging in any unfair, deceptive, or abusive
290 acts or practice in connection with the collection, use, or sharing of personal data. (ii) The
291 agency may prescribe regulations applicable to a data aggregator identifying unlawful, unfair,
292 deceptive, or abusive acts or practices in connection with the collection, use, or sharing of
293 personal data, which may include requirements for the purpose of preventing such acts or
294 practices. Rules under this subsection shall not limit, or be interpreted to limit, the scope of
295 unlawful, deceptive, or abusive acts or practices in connection with the collection, use, or sharing

296 of personal data. (iii) The agency may declare an act or practice in connection with the
297 collection, use, or sharing of personal data to be unlawful on the ground that such act or practice
298 is unfair if the agency has a reasonable basis to conclude that: (A) the act or practice causes or is
299 likely to cause privacy harm or other substantial injury to individuals which is not reasonably
300 avoidable by individuals; and (B) such privacy harm or substantial injury is not outweighed by
301 countervailing benefits to individuals or competition. (iv) The agency may consider established
302 public policies as evidence to be considered with all other evidence but public policy
303 considerations may not serve as a primary basis of such determination. (v) The agency may
304 declare an act or practice abusive in connection with the collection, use, or sharing of personal
305 data if the act or practice: (A) materially interferes with the ability of an individual to understand
306 a term of condition of a good or service; or (B) takes unreasonable advantage of a lack of
307 understanding on the part of the individual of the material risks, costs, or conditions of the
308 product or service; the inability of the individual to protect their interests in selecting or using a
309 product or service; or the reasonable reliance by the individual on a data aggregator or service
310 provider to act in the interests of the individual; and (vi) The agency may limit or require the
311 divestment of any lines of business in which any data aggregator participates based on antitrust
312 or competition concerns and have the authority to review and approve any merger between a data
313 aggregator and any other company whose business is conducted in Massachusetts.

314 (g) It shall be unlawful for; (i) any data aggregator or service provider to commit any act
315 or omission in violation of this chapter or other data privacy law; or to engage in any unfair,
316 deceptive, or abusive act or practice relating to personal data; (ii) any data aggregator or service
317 provider to fail or refuse, as required by this chapter or other privacy law, or any rule or order
318 issued by the agency thereunder to: (A) permit access to or copying of records; (B) establish or

319 maintain records; or (C) to make reports or provide information to the agency; or (iii) any person
320 to knowingly or recklessly provide substantial assistance to a data aggregator or service provider
321 in violation of this section or other data privacy laws, or any rule issued thereunder, and
322 notwithstanding any provision of this act, the provider of such substantial assistance shall be
323 deemed to be in violation of this chapter or other law to the same extent as the person whom
324 substantial assistance is provided.

325 Section 4. Agency Enforcement.

326 (a) The agency or, where appropriate, an agency investigator, may engage in independent
327 or joint investigations and requests for information, as authorized under this chapter.

328 (b) The authority under subsection (a), includes matters relating to protection of
329 individuals' civil rights under this chapter and joint investigations with, and requests for
330 information from, the Consumer Financial Protection Bureau, the Federal Trade Commission,
331 the Department of Health and Human Services, the Department of Education, the office of the
332 United States Attorney General, the office of the Massachusetts Attorney General, the
333 Massachusetts executive office of health and human services, the Massachusetts department of
334 public health, and all other federal and state agencies with oversight of data privacy to promote
335 consistent regulatory treatment across all governmental bodies.

336 (c) The agency, commissioner, employee, or agency investigator may issue subpoenas for
337 the attendance and testimony of witnesses and the production of relevant papers, books,
338 documents, or other material in connection with hearings or investigations under this chapter.

339 (d) In the case of contumacy or refusal to obey a subpoena issued by the agency, pursuant
340 to this section, and served upon any person, the Superior Court of Massachusetts, upon

341 application by the agency, commissioner, employee, or agency investigator and after notice to
342 such person, may issue an order requiring such person to appear and give testimony or to appear
343 and produce documents or other material. Any failure to obey an order of the court under this
344 section may be punished by the court as contempt thereof.

345 (e) The agency may conduct hearings, adjudicatory proceedings, write advisory rulings,
346 and promulgate regulations in accordance with chapter 30A.

347 (f) The Massachusetts Superior Court shall have jurisdiction over all appeals of agency
348 adjudicatory rulings and decisions.

349 (g) Whenever the agency has reason to believe that any person may be in possession,
350 custody, or control of any private data, documentary material or tangible things, or may have any
351 information, relevant to a violation of this chapter, the agency may issue in writing, and cause to
352 be served upon such person, a civil investigative demand, consistent with Chapter 93A of the
353 Massachusetts General Laws, and in coordination with the Massachusetts attorney general's
354 office.

355 (h) Whenever any person fails to comply with any civil investigative demand duly served
356 upon such person, under this section, or whenever satisfactory copying or reproduction of
357 material requested pursuant to the demand cannot be accomplished and such person refuses to
358 surrender such material, the agency, in coordination with the Massachusetts attorney general's
359 office, through such officers or attorneys as it may designate, may file, in Superior Court for an
360 order of the court to enforce this chapter.

361 (i) If, in the opinion of the agency, any data aggregator is engaging or has engaged in an
362 activity that violates a law, rule, or any condition imposed in writing on the person by the

363 agency, the Agency may issue and serve upon the data aggregator or service provider a notice of
364 charges in respect thereof. The notice shall contain a statement of facts constituting the alleged
365 violation or violations, and shall fix a time and place at which a hearing will be held to determine
366 whether an order to cease and desist should issue against the data aggregator or service provider.
367 Such hearing shall be held not earlier than 30 days nor later than 60 days after the date of service
368 of such notice, unless an earlier or later date is set by the agency, at the request of the party
369 served.

370 (j) If the agency finds that any violation specified in the notice of charges has been
371 established, the Agency may issue and serve upon the data aggregator or service provider an
372 order to cease- and-desist from the violation or practice. Such order may, by provisions which
373 may be mandatory or otherwise, require the data aggregator or service provider to cease and
374 desist from the subject activity, and to take affirmative action to correct the conditions resulting
375 from any such violation.

376 (k) The agency may at any time, upon such notice and in such manner as the agency shall
377 determine proper, modify, terminate, or set aside any such order. Upon filing of the record as
378 provided, the agency may modify, terminate, or set aside any such order with permission of the
379 court.

380 (l) Data aggregators, service providers, and persons may appeal a cease-and-desist order
381 to the Superior Court within 10 days of being served such order.

382 (m) The agency may issue a temporary order requiring: (i) the cessation of any activity or
383 practice which gave rise, whether in whole or in part, to the incomplete or inaccurate state of the

384 books or records; or (ii) affirmative action to restore such books or records to a complete and
385 accurate state, until the completion of the proceedings.

386 (n) The agency in its discretion may apply to the Superior Court for the enforcement of
387 any effective and outstanding notice or order issued under this section, and such court shall have
388 jurisdiction and power to order and require compliance with this chapter.

389 (o) If any person violates this act, the agency may commence a civil action against such
390 person to impose a civil penalty or to seek all appropriate legal and equitable relief including a
391 permanent or temporary injunction as permitted by law. The agency may act in its own name and
392 through its own attorneys in enforcing any provision of this chapter.

393 (p) The agency may compromise or settle any action if such compromise is approved by
394 the Superior Court.

395 (q) The agency shall notify the attorney general concerning any action, suit, or
396 proceeding to which the agency is a party and shall consult regarding the coordination of
397 investigations and proceedings, including by negotiating an agreement for coordination on
398 investigations and proceedings.

399 (r) In an action or adjudication proceeding brought under this chapter, the court or the
400 agency shall have jurisdiction to grant any appropriate legal or equitable relief with respect to a
401 violation of this chapter or regulations promulgated through this chapter. Relief under this
402 section shall include, but not be limited to: (i) rescission or reformation of contracts; (ii) refund
403 of moneys or return of real property; (iii) restitution; (iv) disgorgement or compensation for
404 unjust enrichment; (v) payment of damages or other monetary relief; (vi) public notification

405 regarding the violation, including the costs of notification; (vii) limits on the activities or
406 functions of the person; and (viii) civil money penalties.

407 (s) The agency, attorney general's office and any other agency or division of the
408 commonwealth may recover the costs in connection with prosecuting such action if the agency is
409 the prevailing party in the action.

410 (t) Any person that violates, through any act or omission, any provision of this chapter
411 shall forfeit and pay a civil penalty: (i) for any violation of a law, rule, or final order or condition
412 imposed in writing by the agency, a civil penalty may not exceed \$5,000 for each day during
413 which such violation or failure to pay continues; (ii) notwithstanding clause (i), for any person
414 that recklessly engages in a violation of this chapter, a civil penalty may not exceed \$25,000 for
415 each day during which such violation continues; and (iii) any person that re-identifies, or
416 attempts to re-identify, anonymized data shall be assessed a fine of \$25,000 per attempt, not to
417 exceed \$1,000,000 per day.

418 (u) In determining the amount of any penalty assessed under this section, the agency or
419 court shall take into account the appropriateness of the penalty with respect to: (i) the size of
420 financial resources and good faith of the person charged; (ii) the gravity of the violation or
421 failure to pay; (iii) the severity of the risks of harms to the individual; (iv) the history of previous
422 violations; and (v) such other matters as justice may require.

423 (v) The agency may compromise, modify, or remit any penalty which may be assessed or
424 had already been assessed under this chapter.

425 (w) If the agency obtains evidence that any person has engaged in conduct that may
426 constitute a violation of this chapter or other privacy laws, the agency shall transmit such

427 evidence to the Massachusetts attorney general who may institute criminal proceedings under the
428 appropriate law.

429 Section 5. Agency Offices and Departments.

430 (a) The commissioner shall establish offices, divisions or departments within the agency
431 that shall include, but not be limited to an office of: (i) Civil Rights; (ii) Complaints; (iii)
432 Enforcement; and (iv) Data Privacy Research.

433 (b) The office of Civil Rights shall: (i) provide oversight and enforcement of this chapter
434 to ensure that the collection, use, and sharing of personal data is fair, equitable, and
435 nondiscriminatory; (ii) coordinate the agency's civil rights efforts with other federal agencies,
436 state agencies, regulators and constitutional officers to promote consistent, efficient, and
437 effective enforcement of federal and state civil rights laws; (iii) work with civil rights and data
438 privacy organizations and industry to promote compliance with civil rights compliance under this
439 act; and (iv) file annual reports with the office of the governor, attorney general, treasurer and
440 receiver-general and publish these reports online on the agency's website.

441 (c) The complaints division shall manage all consumer complaints from individuals who
442 allege privacy harm by data aggregators. The commissioner shall establish within the complaints
443 division a single toll-free telephone number, a publicly available website, and a publicly
444 available database, to facilitate the centralized collection of, monitoring of, and response to
445 complaints regarding the collection, use, and sharing of personal data.

446 (d) The enforcement division shall: (i) manage all investigations; (ii) work with legal
447 counsel on all adjudicatory proceedings, subpoenas, notice of charges, cease-and-desist orders,
448 and appeals.

449 (e) The data privacy research division shall study, analyze and report on developments
450 regarding data privacy, data collection and use of personal data, study of automated decision
451 systems and all other pertinent topics relative to the improvement of individual's data privacy in
452 the state.

453 Section 6. Website and Database.

454 (a) The agency shall create and maintain a publicly available website and database
455 through which data aggregators shall report the types of personal data that those data aggregators
456 collect, use, or share and an individual may exercise rights, established under this chapter, with
457 respect to the personal data of the individual.

458 (b) The agency shall maintain a publicly accessible list of data aggregators that collect,
459 use, or share personal data of more than 10,000 persons or households, and the permissible
460 purposes for which the data aggregators purport to collect personal data.

461 (c) The agency shall order that the landing page of the agency's main website contain a
462 clear and conspicuous hyperlink to the complaint database and shall: (i) order that such database
463 is user-friendly and in plain writing; (ii) ensure that all complaints are available to the public and
464 shall place a clear and conspicuous hyperlink on the landing page of the main website of the
465 agency that contains a searchable and sortable list of complaints; provided, that the complaints
466 available to the public shall have all personal data removed; (iii) ensure that the website explains
467 how to file a complaint with the agency, where to find reports of the agency, what offices are
468 within the agency, the offices or division's responsibilities, what research has been conducted by
469 the agency, the results of the research and why the research was conducted; and (iv) translate all

470 consumer guidance documents on the agency's website into the five most common languages
471 spoken in Massachusetts.

472 Section 7. Funding Penalties and Fines.

473 (a) There shall be on the books of the commonwealth a fund titled the Data
474 Accountability Fund. The commissioner may collect an assessment, fee, or other charge from a
475 data aggregator that has annual gross revenues that exceed \$25,000,000, or annually collects,
476 uses, or shares, alone or in combination, the personal data of 50,000 or more individuals,
477 households or devices; and provided further, that the commissioner shall determine the manner
478 of payment, and disbursement expenses allowed.

479 (b) 50 per cent of the amounts transferred to the agency under paragraph (a) shall be
480 deposited into the Data Accountability Fund which may be used by the commissioner in
481 accordance with this act.

482 (c) There shall be a separate fund on the books of the commonwealth that shall be titled
483 the Data Relief Fund that shall be established and maintained to assist relief for individuals
484 harmed by data aggregators.

485 (d) 50 per cent of the amounts transferred to the agency under paragraph (a) shall be
486 deposited into the Data Relief Fund.

487 (e) By a majority vote, the board of governors shall determine the investment in the Data
488 Relief Fund money and disbursement to individuals who were victims of privacy harm.

489 (f) No amount transferred to the agency under paragraph (a) shall be deposited into the
490 general fund.

491 Section 8. Annual Reports.

492 (a) The agency shall file annual reports with the office of the governor, attorney general,
493 treasurer and receiver-general and publish these annual reports online, on the agency's website.

494 (b) The annual report shall include: (i) a discussion of the significant problems faced by
495 individuals in exercising their rights under this act; (ii) a justification of the budget request of the
496 previous year; (iii) a list of significant rules and orders adopted by the agency, as well as other
497 significant initiatives conducted by the agency, during the preceding year and plan of the agency
498 for rules, orders, or other initiatives to be undertaken during the upcoming period; (iv) analysis
499 of complaints about practices relating to the collection, use, or sharing of protected data that the
500 agency has received and collected in its central database on complaints during the preceding
501 year; (v) a list, with a brief statement of issues of the public supervisory and enforcement actions
502 to which the agency was a party during the preceding year; (vi) the actions taken regarding rules,
503 orders, and supervisory actions with respect to data aggregators; (vii) an assessment of
504 significant actions by the Massachusetts attorney general, state attorneys general or other state
505 regulators relating to this chapter; (viii) an analysis of the efforts of the agency to fulfill the civil
506 rights in data mission of the agency; and (ix) and analysis of the efforts of the agency to increase
507 workforce and contracting diversity.

508 Section 9. Requirements for Data Aggregators.

509 (a) Data aggregators shall not collect, use, or share, or cause to be collected, used, or
510 shared any personal data unless the data aggregator can demonstrate that such personal data is
511 strictly necessary to carry out a permissible purposed under subsection (b).

512 (b) A data aggregator may not collect, use, or share personal data unless strictly necessary
513 to carry out one or more of the following permissible purposes: (i) to provide a good, service, or
514 specific feature requested by an individual in an intentional interaction; (ii) to engage in
515 journalism, provided that the data aggregator has reasonable safeguards and processes that
516 prevent the collection, use, or sharing of personal data; (iii) to conduct public or peer-reviewed
517 scientific, historical, or statistical research in the public interest, but only to the extent such
518 research is not possible using anonymized data; (iv) to employ an individual, including for
519 administration of wages and benefits, except that a data aggregator may not invasively collect,
520 use, or share the employee’s personal data in carrying out this paragraph; (v) to comply with law;
521 (vi) consistent with due process, direct compliance with a civil, criminal, or regulatory inquiry,
522 investigation, subpoena or summons; (vii) to bring or defend legal claims, provided that the
523 parties or potential parties take all necessary measures, including, as applicable, obtaining a
524 protective order, to protect against unnecessary public disclosure of personal data; (viii) to detect
525 or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal
526 activity, or prosecute those responsible for that activity; (ix) free expression by individuals on a
527 social network or media platform; (x) in exigent circumstances, if first responders or medical
528 personnel, in good faith, believe danger of death or serious physical injury to an individual, or
529 danger of serious and unlawful injury to property, requires collection, use, or sharing of personal
530 data relating to the exigent circumstances; (xi) the development and delivery of advertisements:
531 (A) based on the content of the website, online service, or application to which the individual or
532 device is connected; and (B) excludes advertizing based on the use of any personal data collected
533 or stored from previous interactions with the individual or device, a profile of the individual or
534 device, or the previous online or offline behavior of the individual or device; or (xii) to offer

535 discounted or free goods or services to an individual if: (A) the offering is in connection with the
536 voluntary participation by the individual in a program that rewards patronage; and (B) personal
537 data is only collected to track purchases for loyalty rewards under the program described in (A).

538 (c) Except where strictly necessary to carry out a permissible purpose, a data aggregator
539 shall not: (i) share personal data with affiliated entities, service providers, or third parties; (ii) use
540 personal data for any purpose other than to carry out a permissible purpose; (iii) retain personal
541 data for longer than strictly necessary to carry out a permissible purpose; or (iv) derive or infer
542 data from any element or set of personal data; and (v) collecting, using, or sharing personal data
543 to generate advertising revenue to support or carry out a permissible purpose is not a permissible
544 purpose.

545 (d)(i) It is unlawful for a person to engage or cause to be engaged in the following
546 practices: (A) charge an extra fee or raise the price for a good, service, or feature when a person
547 exercises the rights of the person under this chapter; (B) terminate, refuse to provide, degrade
548 goods or services to, or otherwise retaliate against, a person that exercises the rights of the person
549 under this act; (C) re-identify, or attempt to re-identify, an individual, household, or device from
550 anonymized data, unless conducting authorized testing to prove personal data has been
551 anonymized; and (D) commingle personal data from multiple applications, services, affiliates, or
552 independent business lines. (ii) It is unlawful for any data aggregator to: (A) use facial
553 recognition technology; or (B) collect, use or share any personal data obtained from facial
554 recognition technology. (iii) A person is prohibited from engaging in the unlawful data practices
555 in paragraph (d)(i) regardless of whether such person has a permissible purpose for collecting,
556 using, or sharing personal data. (iv) In addition to relief available under section 14, a data
557 aggregator shall be subject to treble damages for a violation of this section.

558 (e) It shall be unlawful for a data aggregator to collect, use, or share personal data for
559 advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise
560 commercially contracting for housing, employment, credit, or insurance in a manner that
561 discriminates against or otherwise makes the opportunity unavailable or offered on different
562 terms on the basis of a protected class or otherwise materially contributes to unlawful
563 discrimination.

564 (f) It shall be unlawful for a data aggregator to collect, use, or share personal data in a
565 manner that segregates, discriminates in, or otherwise makes unavailable the good, services,
566 facilities, privileges, advantages, or accommodations of any place of public accommodation on
567 the basis of a protected class.

568 (g) It shall be unlawful for a data aggregator to: (i) withhold, deny, deprive, or attempt to
569 withhold, deny, or deprive any individual of any right or privilege secured by this chapter; (ii)
570 intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any individual with
571 the purpose of interfering with any right or privilege secured by this section; or (iii) punish or
572 attempt to punish any individual for exercising or attempting to exercise any right or privilege
573 secured by this section.

574 (h) It shall be unlawful for a person to use personal data in a manner that deprives,
575 defrauds, or attempts to deprive or defraud an individual of the free and fair exercise of the right
576 to vote in a Federal, State, or local election. Intentionally depriving or attempting to
577 deprive or defraud includes: (i) deception as to the times, places, or methods of voting; eligibility
578 to vote; counting of ballots; adjudications of elections; explicit endorsements by any person of a
579 candidate; or other material information pertaining to the procedures or requirements for voting

580 or registering to vote in a Federal, State, or local election; or (ii) using deception, threats,
581 intimidation, or coercion to prevent, interfere with, retaliate against, deter, or attempt to prevent,
582 interfere with, retaliate against, or deter: (A) voting or registering to vote in a Federal, State, or
583 local election; or (B) giving support or advocacy in a legal manner toward a candidate in a
584 Federal, State, or local election.

585 (i) It shall be unlawful for any data aggregator to discriminate against an individual
586 because the individual exercised any of their rights under this chapter, or did not agree to the use
587 of their personal data for a separate product or service, including by: (i) denying goods or
588 services; (ii) charging different prices or rates for goods or services, including through the use of
589 discounts or other benefits or imposing penalties; (iii) providing a different level or quality of
590 goods or services; and (iv) suggesting that an individual will receive a different price or rate for
591 goods or services or a different level or quality of goods or services.

592 (j) If the use of personal data causes a disparate impact on the basis of a protected class
593 under this section, the data aggregator has the burden of demonstrating that such use of personal
594 data: (i) is not intentionally discriminatory; (ii) is strictly necessary to achieve one or more
595 substantial, legitimate, nondiscriminatory interests; and (iii) there is no reasonable alternative
596 policy or practice that could serve the interest described in paragraph (ii) with a less
597 discriminatory effect.

598 Section 10. Algorithmic Accountability.

599 (a) If a data aggregator utilizes automated decision systems, the data aggregator shall
600 perform: (i) continuous and automated testing for bias on the basis of a protected class; and (ii)

601 continuous and automated testing for disparate impact on the basis of a protected class as
602 required by the agency.

603 (b) When evaluating an automated decision system against other less discriminatory
604 alternative, similar methodology shall be used to create the alternatives.

605 (c) For any automated decision system, a data aggregator shall provide the agency: (i) an
606 automated decision system risk assessment, within 90 days for any automated decision system
607 currently in use; prior to the deployment of any new automated decision system; or as
608 determined by the commissioner; and (ii) an automated decision system impact evaluation on a
609 periodic basis as determined by the commissioner, but no less than annually.

610 (d) The agency shall make automated decision system impact evaluations publicly
611 available and shall be published on the agency's website.

612 Section 11. Individual Rights.

613 (a) Upon receipt of a verifiable request, a data aggregator shall provide the: (i) specific
614 pieces of personal data collected, used, or shared about the individual; (ii) permissible purposes
615 for such collection, use, or sharing of an individual's personal data at the time of collection, use,
616 or sharing; (iii) service providers or third parties with which it has shared the personal data; and
617 (iv) individual's personal data in an electronic, portable, machine-readable, and readily useable
618 format or formats to the individual, or to another person of the individual's choice.

619 (b) A data aggregator shall disclose the following information, including in its online
620 privacy policy: (i) a description of an individual's rights under this chapter and designated
621 methods for submitting verifiable requests; (ii) a description of the personal data that the data

622 aggregator collects, uses, or shares; (iii) the specific sources from which personal data is
623 collected; (iv) a description of the sources from which personal data is collected; (v) the
624 permissible purposes for which personal data is collected, used, or shared; (vi) the affiliates,
625 service providers, or third parties with which the data aggregators shares personal data, and the
626 permissible purpose for such sharing; (vii) a description of the length of time for which personal
627 data is retained; and (viii) if personal data is collected and retained as anonymized data, a
628 description of the techniques and methods used to create the anonymized data.

629 (c) A data aggregator shall maintain reasonable policies and procedures to ensure that any
630 personal data that it collects, uses or shares is accurate. An individual has the right to require that
631 a data aggregator that retains the individual's personal data correct any inaccurate or incomplete
632 personal data. Upon receipt of a verifiable request, a data aggregator shall correct and inaccurate
633 or incomplete personal data, as directed by that individual, and direct any service provider to
634 correct the individual's personal data in its records.

635 (d) An individual has the right to request that a data aggregator delete any personal data
636 that the data aggregator has collected about the individual. Unless strictly necessary to carry out
637 a permissible purpose under Section 9, upon receipt of a verifiable request, a data aggregator
638 shall delete the personal data of such individual, and direct any service providers to delete such
639 individual's personal data from its records.

640 (e) An individual has the right to object to the claimed permissible purpose for any
641 personal data that a data aggregator has collected, used, or shared of such individual. Upon
642 receipt of an individual's verifiable request that objects to the data aggregator's claimed
643 permissible purpose for collecting, using, or sharing such individual's personal data, a data

644 aggregator shall produce evidence supporting the data aggregator’s claim that the collection, use,
645 or sharing of such individual’s personal data: (i) was strictly necessary to carry out a permissible
646 purpose; (ii) was not used or shared for any other purpose; and (iii) has not been retained for any
647 time longer than strictly necessary to carry out a permissible purpose.

648 (f) For any material decision by a data aggregator based on automated processing of
649 personal data of an individual, a data aggregator shall: (i) inform the individual of the specific
650 personal data that was used for such a decision; (ii) make available an easily available
651 mechanism by which the individual may request human review of such decisions; and (iii) upon
652 receipt of a verifiable request for a human review of material decision, conduct such a review
653 within 15 days of the date of the request.

654 Section 12. Duty of care.

655 (a) A data aggregator shall implement and maintain reasonable security procedures and
656 practices, including administrative, physical, and technical safeguards, appropriate to the nature
657 of the personal data and the purposes for which the personal data will be collected, used, or
658 shared, to ensure that personal data: (i) is only collected, used, or shared where strictly necessary
659 to carry out a permissible purpose under Section 9; (ii) is not retained for any time longer than
660 strictly necessary to carry out a permissible purpose under Section 9; and (iii) is protected from
661 unauthorized collection, use, sharing, or disclosure.

662 (b) A data aggregator: (i) shall ensure that the service providers of the data aggregator
663 comply with the requirements of this chapter; and (ii) is liable for any violation of this chapter by
664 its service providers.

665 Section 13. Duties of Data Aggregator Upon Receipt of Verifiable Request.

666 (a) A data aggregator is prohibited from charging any fee to carry out a verifiable request
667 under this chapter.

668 (b) A data aggregator shall carry out a verifiable request within 30 days of receiving the
669 verifiable request.

670 (c) The requirements of this chapter shall not apply if the data aggregator receiving a
671 verifiable request determines that the verifiable request is frivolous or irrelevant, including by
672 reason of: (i) the failure of the individual to provide sufficient information to carry out the
673 verifiable request; or (ii) the verifiable request is substantially the same as a verifiable request
674 previously submitted by the individual, with respect to which the person has already performed
675 the data aggregator's duties under this chapter.

676 Section 14. Private Right of Action.

677 (a) Any person may commence a civil action: (i) against any person, including the
678 commonwealth of Massachusetts or any other governmental instrumentality or agency to the
679 extent permitted by the Eleventh Amendment to the Constitution of the United States, that is
680 alleged to have violated this chapter; or (ii) against the agency if the agency is alleged to have:
681 (A) adopted a rule in violation of any provision of chapter 30A of the general laws; or any
682 provision of this chapter; or (B) failed to promulgate a rule required under this chapter, in order
683 to compel the issuance of such rule.

684 (b) The Superior Court of Massachusetts shall have jurisdiction over all civil actions in
685 subsection (a).

686 (c) In a civil action brought under (a)(i), in which the plaintiff prevails, the court may
687 award: (i) an amount not less than \$100, and not greater than \$1,000, per violation per day or
688 actual damages, whichever is greater; (ii) punitive damages; (3) reasonable attorney's fees and
689 litigation costs; and (4) any other relief, including a temporary or permanent injunction,
690 equitable, or declaratory relief, that the court determines appropriate.

691 (d) A violation of this chapter or a regulation promulgated under this chapter is presumed
692 to cause privacy harm and constitutes a concrete and particularized injury in fact to that
693 individual.

694 Section 15. Corporate Accountability.

695 (a) Each data aggregator shall establish comprehensive privacy and data security policies,
696 procedures, and practices to ensure compliance with this act.

697 (b) Each data aggregator shall submit to the agency an annual report: (i) describing its
698 collection, use, or sharing of personal data, and the permissible purpose for such collection, use,
699 or sharing of personal data; (ii) identifying each service provider with which the data aggregator
700 shares personal data, the permissible purposes for sharing personal data with each such service
701 provider, and a description of the oversight and supervision conducted by the data aggregator to
702 ensure that each such service provider complies with the requirements of this chapter; (iii)
703 internal controls that the data aggregator has put in place to ensure compliance with the
704 requirements of this chapter; and (iv) a description of the testing, and results of such testing, to
705 ensure compliance with the requirements of this act.

706 (c) The chief executive officer or, if the data aggregator does not have a chief executive
707 officer, the highest ranking officer of the data aggregator, shall annually certify to the agency

708 that it has complied with this chapter, including: (i) conducted oversight sufficient to
709 demonstrate all service providers are complying with this chapter; (ii) maintains adequate
710 internal control sufficient to demonstrate compliance with this chapter; (iii) conducted testing
711 sufficient to demonstrate compliance with this act; and (iv) maintains reporting structures to
712 ensure that the chief executive officer, or if a chief executive officer does not exist, the highest
713 ranking officer that is involved in, and responsible for, decisions to ensure compliance with this
714 chapter.

715 Section 16. Criminal and Civil Penalties for CEO and Board of Directors.

716 (a) Criminal Penalty. Whoever knowingly and intentionally violates, or knowingly and
717 intentionally attempts to violate, sections 9, 10, or 15, shall be fined \$250,000, or imprisoned for
718 not more than five years, or both.

719 (b) Whoever violates, or attempts to violate, sections 9, 10, or 15 while violating another
720 law or as part of a pattern of any illegal activity involving more than \$100,000 in a 12-month
721 period shall be fined twice the amount provided in subsection (a) for individuals and for
722 \$1,000,000 for organizations, or imprisoned for not more than 10 years, or both.

723 (c) Whoever violates this section shall be liable to the state of Massachusetts for a civil
724 fine of not more than \$10,000,000.

725 Section 17. Whistle Blower Protections.

726 (a) A data aggregator may not, directly or indirectly, discharge, threaten, harass, suspend,
727 demote, terminate, or in any other manner discriminate against a covered individual because (i)
728 the covered individual, or anyone perceived as assisting the covered individual, takes, or the data

729 aggregator suspects that the covered individual has taken or will take, a lawful action in
730 providing to the government or the attorney general of Massachusetts information relating to any
731 act or omission that the covered individual reasonably believes to be a violation of this chapter or
732 any regulation promulgated under this chapter; (ii) the covered individual provides information
733 that the covered individual reasonably believes evidences such a violation to: (A) a person with a
734 supervisory authority over the covered individual at the covered entity; or (B) another individual
735 working for the covered entity who the covered entity reasonably believes has the authority to
736 investigate, discover, or terminate the violation or to take any other action to address the
737 violation; (iii) the covered individual testifies, or the covered entity expects that the covered
738 individual will testify, in an investigation or judicial or administrative proceeding concerning
739 such a violation; (iv) the covered individual assists or participates in such an investigation or
740 judicial or administrative proceeding; or (v) take any other action to assist in carrying out the
741 purposes of this chapter.

742 (b) An individual who alleges discharge or other discrimination in violation of subsection
743 (a) may bring an action governed by the rules, procedures, statute of limitations, and legal
744 burdens of proof in section 185 of chapter 149 of the Massachusetts General Laws. If the
745 individual has not received a decision within 180 days and there is no showing of bad faith of the
746 claimant, the individual may bring an action for a jury trial in Massachusetts Superior Court, for
747 the following relief: (i) temporary relief while case is pending; (ii) reinstatement of seniority, but
748 for the discharge or discrimination; (iii) three times the amount of back pay otherwise owed to
749 the individual, with interest; and (iv) consequential and compensatory damages, and
750 compensation for litigation costs, expert witness fees, and reasonable attorneys' fees.

751 Section 18. Waiver of Rights and Remedies.

752 No provisioner of this chapter may be waived and any agreement to waive compliance
753 with or modify any provision of this chapter shall be void as contrary to public policy.

754 Section 19 Severability.

755 If any provision of this chapter or the application of such provision is held to be
756 unconstitutional, the remainder of this chapter, and the application of the provisions of such to
757 any person or circumstances, shall not be affected thereby.

758 SECTION 2. Section 8 of Chapter 223 is hereby amended by striking out the paragraph
759 after the words “the state racing commission,” and inserting the following:-

760 the Massachusetts Data Accountability and Transparency Agency, the parole board or a
761 board of appeals designated or appointed under section thirty of chapter forty, as to matters
762 within their authority; and such witnesses shall be summoned in the same manner, be paid the
763 same fees and be subject to the same penalties for default, as witnesses in civil cases before the
764 courts. The presiding officer of such council, or of either branch thereof, or a member of any
765 such committee, board or commission, or any such commissioner, may administer oaths to
766 witnesses who appear before such council, branch thereof, committee, board, commission or
767 commissioner, or agency respectively.

768 SECTION 3. Section 2 of chapter 32A of the General Laws, as so appearing, is hereby
769 amended by inserting after the words “Massachusetts cannabis control commission”, in lines 13
770 and 14, the following words:- Massachusetts Data Accountability and Transparency Agency,

771 SECTION 4. Section 2 of Chapter 93A of the General Laws, is hereby amended by
772 adding the following subsection:-

773 (d) The attorney general shall coordinate with the Massachusetts Data Accountability and
774 Transparency Agency regarding violations of chapter 93L of the General Laws.

775 SECTION 5. Chapter 12 of the General Laws, is hereby amended by adding the
776 following section:-

777 Section 35.

778 (a) The attorney general shall have the power to enforce all of Chapter 93L in
779 coordination with the Massachusetts Data Accountability and Transparency Agency.

780 (b) The attorney general shall promulgate regulations to enforce this section and Chapter
781 93L.

782 (c) The attorney general shall coordinate with the Massachusetts Data Accountability and
783 Transparency Agency and negotiate an agreement regarding investigations and proceedings.

784 (d) The attorney general shall ensure uniformity in data privacy laws across the state.