

**SENATE . . . . . No.**

---

**The Commonwealth of Massachusetts**

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

An Act establishing the Massachusetts Information Privacy and Security 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 are hereby amended by inserting after Chapter 93L the  
2 following chapter:-

3           CHAPTER 93M. The Massachusetts Information Privacy and Security Act.

4           Section 1. Title

5           This chapter shall be known as the “Massachusetts Information Privacy and Security  
6 Act.”

7           Section 2. Definitions

8           As used in this chapter, the following words shall have the following meanings unless the  
9 context clearly requires otherwise:

10           “Advertising” means a communication in any medium by a controller or an entity acting  
11 on the controller’s behalf intended to induce an individual to obtain goods, services, or  
12 employment.

13           “Affiliate” means an entity that controls, is controlled by, or is under common control or  
14 shares common branding with another entity. For the purposes of this definition, “control” or  
15 “controlled” shall mean: (1) ownership of more than fifty per cent of the outstanding shares of  
16 any class of voting security of the entity; (2) control in any manner over the election of a  
17 majority of the entity’s directors or of persons exercising similar functions; or (3) the power to  
18 otherwise exercise a controlling influence over the management of the entity.

19           “Authorized agent” means an entity or natural person that an individual has designated  
20 pursuant to subSection (d) of Section 15 of this chapter.

21           “Biometric information” means a retina or iris scan, fingerprint, voiceprint, map or scan  
22 of hand or face geometry, vein patterns, gait patterns, or other measurements of unique  
23 biological patterns or characteristics used to identify a specific individual; provided, however,  
24 that “biometric information” shall not include: (i) writing samples; (ii) written signatures; (iii)  
25 photographs; (iv) video or audio recordings or data generated therefrom; (v) human biological  
26 samples used for valid scientific testing or screening; (vi) demographic data; (vii) tattoo  
27 descriptions; (viii) physical descriptions such as height, weight, hair color or eye color; (ix)  
28 donated organs, tissues, or parts as defined in chapter 113A of the General Laws; (x) blood or  
29 serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and  
30 obtained or stored by a federally designated organ procurement agency; (xi) biological materials  
31 regulated under Section 70G of chapter 111 of the General Laws; (xii) information captured from  
32 a patient in a health care setting; (xiii) information collected, used, or stored for health care  
33 treatment, payment or operations under HIPAA; or (xiv) an X-ray, roentgen process, computed  
34 tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used

35 to diagnose, prognose, or treat an illness or other medical condition or to further validate  
36 scientific testing or screening.

37 “Business associate” shall have the same meaning as in 45 C.F.R. 160.103.

38 “Child” means an individual who a controller knows or reasonably should know is under  
39 the age of 13.

40 “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining,  
41 receiving, or otherwise accessing any personal information pertaining to an individual by any  
42 means. This includes, but is not limited to, obtaining information from the individual, either  
43 actively or passively, or by observing the individual’s behavior.

44 “Common branding” means a shared name, servicemark, trademark, or other indicator  
45 that an individual would reasonably understand to indicate that two or more entities are  
46 commonly owned.

47 “Consent” means a clear affirmative act signifying an individual’s freely given, specific,  
48 informed, and unambiguous agreement to allow the processing of personal information relating  
49 to the individual for a narrowly defined particular purpose. Consent may include a written  
50 statement, including a statement written by electronic means, or any other unambiguous  
51 affirmative action. The following shall not constitute consent: (1) acceptance of a general or  
52 broad terms of use or similar document that contains descriptions of personal information  
53 processing along with other, unrelated information; (2) hovering over, muting, pausing, or  
54 closing a given piece of content; or (3) agreement obtained through dark patterns.

55 “Controller” means the entity that, alone or jointly with others, determines the purposes  
56 and means of the processing of personal information of an individual.

57 “Covered entity” shall have the same meaning as in 45 C.F.R. 160.103.

58 “Dark pattern” means a user interface designed or manipulated with the substantial effect  
59 of subverting or impairing user autonomy, decision-making, or choice.

60 “Data broker” means a controller that knowingly collects and sells to third parties:

61 (1) The sensitive information of not less than 10,000 individuals; or

62 (2) The personal information of not less than 10,000 individuals with whom the controller  
63 does not have a direct relationship, including, but not limited to, a relationship in which an  
64 individual is a past or present: (i) customer, client, subscriber, user, or registered user of the  
65 controller’s goods or services; (ii) an employee, contractor, or agent of the controller; (iii) an  
66 investor in the controller; or (iv) a donor to the controller.

67 The following activities conducted by a controller, and the collection and sale of personal  
68 information incidental to conducting these activities, shall not qualify the controller as a data  
69 broker: (i) providing 411 directory assistance or directory information services, including name,  
70 address, and telephone number, on behalf of or as a function of a telecommunications carrier; (ii)  
71 providing publicly available information related to an individual’s business or profession; or (iii)  
72 providing publicly available information via real-time or near-real-time alert services for health  
73 or safety purposes.

74 “De-identified information” means information, derived from personal information, that  
75 cannot reasonably be used to infer information about, or otherwise be linked to, an identified or

76 identifiable individual or household, or a device linked to such individual or household. De-  
77 identification means the creation of de-identified information from personal information.

78 “Designated methods for submitting a request” means a mailing address, email address,  
79 Internet web page, Internet web portal, toll-free telephone number, or other applicable contact  
80 information, whereby an individual may submit a request or direction under this chapter,  
81 provided that: (1) the designated methods shall be reasonably accessible to individuals and take  
82 into account the ways in which individuals interact with the controller, the need for secure and  
83 reliable communication of the request, and the ability of the controller to determine that the  
84 request is a verifiable request; and (2) a controller shall not require an individual to create a new  
85 account in order to exercise a right under this chapter, but a controller may require an individual  
86 to use an existing account to exercise the individual’s rights under this chapter.

87 “Device” means any physical object that is capable of connecting to the Internet, directly  
88 or indirectly, or to another device.

89 “Entity” means a sole proprietorship, or a corporation, association, partnership or other  
90 legal entity.

91 “Health care facility” shall have the same meaning as defined in Section 25B of chapter  
92 111 of the General Laws.

93 “Health care provider” shall have the same meaning as defined in Section 1 of chapter  
94 111 of the General Laws.

95 “Health record” means an individual’s health-related record, as kept pursuant to Section  
96 70 of chapter 111 of the General Laws.

97 “HIPAA” means the federal Health Insurance Portability and Accountability Act of 1996,  
98 42 U.S.C. 1320d et seq., as amended from time to time.

99 “Homepage” means the introductory page of an Internet website and any Internet web  
100 page where personal information is collected; provided, however, that in the case of an online  
101 service, such as a mobile application, homepage shall mean: (i) the application’s platform page  
102 or download page; (ii) a link within the application, such as from the application configuration,  
103 “About,” “Information,” or settings page; or (iii) any other location that allows individuals to  
104 review the notices required by this chapter, including, but not limited to, before downloading the  
105 application.

106 “Identified or identifiable individual household” is a group of individuals who: (i)  
107 cohabitate with one another at the same residential address in the Commonwealth; (ii) use  
108 common devices or services; and (iii) can be readily identified, directly or indirectly.

109 “Identified or identifiable individual” means an individual who can be readily identified,  
110 directly or indirectly.

111 “Individual” means a natural person who is a resident of the Commonwealth; provided,  
112 however, that “individual” shall not include a natural person acting as a sole proprietorship.

113 “Infer” or “inference” means the derivation of information, data, assumptions or  
114 conclusions from facts, evidence, or another source of information or data.

115 “Institution of higher education” means any college, junior college, university or other  
116 public or private educational institution that has been authorized to grant degrees pursuant to  
117 Sections 30, 30A, and 31A of chapter 69 of the General Laws.

118 “Intentionally interacts” means when an individual intends to interact with an entity, or  
119 disclose personal information to an entity, via one or more deliberate interactions, including  
120 visiting the entity’s website or purchasing a good or service from the entity; provided, however,  
121 that hovering over, muting, pausing, or closing a given piece of content does not constitute an  
122 individual’s intent to interact with an entity.

123 “Minor” means an individual who a controller knows or reasonably should know is not  
124 less than 13 years of age and not more than 16 years of age.

125 “Nonpersonalized advertising” means advertising that is based solely on an individual’s  
126 personal information, except for the individual’s specific geolocation information, derived from  
127 the individual’s current interaction with the controller.

128 “Nonprofit organization” means any organization that is exempt from taxation under 26  
129 U.S.C. 501(c), as amended from time to time.

130 “Personal information” means information that identifies, relates to, describes, is  
131 reasonably capable of being associated with, or could reasonably be linked, directly or indirectly,  
132 with an identified or identifiable individual; provided, however, that personal information shall  
133 not include de-identified information or publicly available information.

134 For the following purposes, personal information shall also include information that  
135 identifies, relates to, describes, is reasonably capable of being associated with, or could  
136 reasonably be linked, directly or indirectly, with an identified or identifiable household:

137 (1) As “personal information” is used in the definition of “sale,” “sell” or “sold” in this  
138 Section;

139 (2) In any other reference to the sale of personal information in this chapter; or

140 (3) As “personal information” is used in subSection (b) of Section 3 of this chapter.

141 “Process” or “processing” means any operation or set of operations which are performed  
142 on personal information or on sets of personal information, whether or not by automated means,  
143 such as the collection, use, storage, disclosure, analysis, prediction, deletion, or modification of  
144 personal information. Process or processing includes the actions of a controller directing a  
145 processor to process personal information.

146 “Processor” means an entity that processes personal information on behalf of a controller.

147 “Protected health information” shall have the same meaning as defined in 45 C.F.R.  
148 160.103, established pursuant to HIPAA.

149 “Publicly available information” means information about an individual that is: (1)  
150 lawfully made available from federal, state, or local government records; or (2) information that  
151 a controller has a reasonable basis to believe is lawfully and intentionally made available by the  
152 individual to the general public through widely distributed media.

153 “Research” means a systematic investigation, including research development, testing,  
154 and evaluation, designed to develop or contribute to generalizable knowledge and that is  
155 conducted in accordance with other applicable ethics and privacy laws.

156 “Sale, “sell,” or “sold” means sharing, renting, releasing, disclosing, disseminating,  
157 making available, transferring, or otherwise communicating orally, in writing, or by electronic or  
158 other means, an individual’s personal information by the controller to a third party for monetary



159 or other valuable consideration in a bargained-for exchange, or for the purposes of targeted  
160 advertising. “Sale,” “sell,” or “sold” does not include the following:

161 (1) The disclosure of personal information to a processor where the processor only  
162 processes such personal information on behalf of the controller;

163 (2) The controller’s use or sharing of an identifier for an individual who has opted out of  
164 the sale of the individual’s personal information or limited the use of the individual’s sensitive  
165 information for the purposes of alerting entities that the individual has opted out of the sale of the  
166 individual’s personal information or limited the use of the individual’s sensitive information;

167 (3) The disclosure or transfer of personal information to an affiliate of the controller;

168 (4) The disclosure or transfer of personal information to a third party as an asset that is  
169 part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the  
170 third party assumes control of all or part of the controller’s assets;

171 (5) The disclosure of personal information to a third party for purposes of providing a  
172 product or service specifically requested by the individual; or

173 (6) When the individual uses or expressly directs the controller to disclose personal  
174 information to a third party or otherwise interact with a third party, not including disclosures or  
175 interactions for the purposes of targeted advertising; provided, however, that the individual’s  
176 direction was not obtained through dark patterns.

177 “Security and integrity” means the ability of:

178 (1) Networks or information systems to detect security incidents that compromise the  
179 availability, authenticity, integrity, and confidentiality of stored or transmitted personal  
180 information;

181 (2) Controllers to detect security incidents, resist malicious, deceptive, fraudulent or  
182 illegal actions and to help prosecute those responsible for those actions; or

183 (3) Controllers to ensure the physical safety of natural persons.

184 “Sensitive information” means:

185 (1) Personal information that reveals an individual’s: (i) racial or ethnic origin, (ii)  
186 religious beliefs; or (iii) citizenship or immigration status;

187 (2) Biometric information or genetic information processed for the purpose of uniquely  
188 identifying an individual;

189 (3) Personal information processed concerning an individual’s mental or physical health  
190 diagnosis or treatment;

191 (4) Personal information processed concerning an individual’s sex life or sexual  
192 orientation;

193 (5) An individual’s specific geolocation information;

194 (6) The personal information from a child;

195 (7) Personal information that reveals an individual’s philosophical beliefs or union  
196 membership; or

197 (8) Personal information that reveals: (i) an individual’s social security number, driver’s  
198 license number, military identification number, passport number, or state-issued identification  
199 card number; or (ii) financial account number, or credit or debit card number, with or without  
200 any required security code, access code, personal identification number or password, that would  
201 permit access to an individual’s financial account.

202 Sensitive information is a form of personal information. Sensitive information that is  
203 “publicly available information” shall not be considered sensitive information or personal  
204 information.

205 “Specific geolocation information” means information derived from technology  
206 including, but not limited to, global positioning system level latitude and longitude coordinates  
207 or other mechanisms that directly identify the specific location of an individual within a  
208 geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.  
209 Specific geolocation information excludes the content of communications or any information  
210 generated by or connected to advanced utility metering infrastructure systems or equipment for  
211 use by a utility.

212 “Targeted advertising” means the targeting of advertising to an individual based on the  
213 individual’s personal information obtained from the individual’s activity across controllers,  
214 distinctly-branded websites, applications, or services, other than the controller, distinctly-  
215 branded website, application, or service with which the individual intentionally interacts.

216 Targeted advertising shall not include:

217 (1) Advertising to an individual in response to the individual’s request for information  
218 and feedback;

219 (2) Advertising based on the context of an individual’s current search query, visit to a  
220 website, or online application; or

221 (3) Processing personal information solely for measuring or reporting advertising  
222 performance, reach, or frequency.

223 “Third party” means a natural person, entity, public authority, agency, or body other than  
224 the applicable individual, controller, processor, or affiliate of the controller or the processor.

225 “Verifiable request” means a request: (i) to exercise any of the rights set forth in Sections  
226 8 through 11 of this chapter; and (ii) that a controller can use commercially reasonable means to  
227 determine is being made by the individual or by a person authorized to exercise rights on behalf  
228 of such individual with respect to the personal information at issue, pursuant to subSections (b)  
229 and (c) of Section 15 of this chapter.

### 230 Section 3. Scope and Applicability

231 (a) This chapter shall apply to:

232 (1) A controller or processor that conducts business in the Commonwealth; and

233 (2) The processing of personal information by a controller or processor not physically  
234 established in the Commonwealth, where the processing activities are related to: (i) the offering  
235 of goods or services that are targeted to individuals; or (ii) the monitoring of behavior of  
236 individuals where such behavior takes place in the Commonwealth.

237 (b) Notwithstanding subSection (a) of this Section, Sections 7 through 17 and Section 20  
238 of this chapter shall only apply to a controller that satisfies at least 1 of the following additional  
239 thresholds or is an entity that is an affiliate of and shares common branding with such a

240 controller, in which case Sections 7 through 17 and Section 20 shall apply only to the personal  
241 information processed by the affiliate on behalf of the controller:

242 (1) The controller, as of January 1 of the calendar year, had annual global gross revenues  
243 in excess of 25,000,000 dollars in the preceding calendar year;

244 (2) The controller determines the purposes and means of processing of the personal  
245 information of not less than 100,000 individuals; or

246 (3) The controller is a data broker.

247 (c) Payment-only credit, check, or cash transactions where no information is retained  
248 about an individual entering into the transaction do not count as “individuals” for the purposes of  
249 subSection (b).

250 (d) The provisions of this chapter are not limited to personal information collected  
251 electronically or over the Internet, but apply to the processing of all personal information  
252 processed by a controller.

253 (e) This chapter shall not apply to:

254 (1) Any agency, executive office, department, board, commission, bureau, division or  
255 authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

256 (2) Any national securities association that is registered under 15 U.S.C. 78o-3 of the  
257 Securities Exchange Act of 1934, as amended from time to time.

258 (3) Any registered futures association that is so designated pursuant to 7 U.S.C. 21, as  
259 amended from time to time.

260 (f) The following information shall be exempt from the provisions of this chapter:

261 (1) Protected health information that is processed by a covered entity or business  
262 associate pursuant to 45 C.F.R. 160, 162, and 164.

263 (2) Health records for the purposes of Section 70 of chapter 111 of the General Laws, to  
264 the extent that the records are maintained pursuant to 45 C.F.R. 160, 162, and 164.

265 (3) Information and documents that are created by a covered entity for purposes of  
266 complying with HIPAA and its implementing regulations.

267 (4) Information used only for public health activities and purposes as authorized by  
268 HIPAA.

269 (5) Patient identifying information for purposes of 42 C.F.R. 2, established pursuant to 42  
270 U.S.C. 290dd-2, as amended from time to time.

271 (6) Information that is: (i) collected for a clinical trial subject to the Federal Policy for the  
272 Protection of Human Subjects (also known as the Common Rule) under 45 C.F.R. 46; (ii)  
273 collected pursuant to good clinical practice guidelines issued by the International Council for  
274 Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; (iii) collected  
275 pursuant to the human subject protection requirements under 21 C.F.R. 50 and 56; or (iv)  
276 personal information used or disclosed in research conducted in accordance with one or more of  
277 the requirements set forth in this paragraph.

278 (7) Information and documents created for purposes of the federal Health Care Quality  
279 Improvement Act of 1986, 42 U.S.C. 11101 et seq., as amended from time to time.

280 (8) Patient safety work product for purposes of the federal Patient Safety and Quality  
281 Improvement Act, 42 U.S.C. 299b-21 et seq., as amended from time to time.

282 (9) Information that is: (i) derived from any of the health care-related information listed  
283 in this subSection; and (ii) de-identified in accordance with the requirements for de-identification  
284 pursuant to 45 C.F.R. 164.

285 (10) Information that is treated in the same manner as, or that originates from and is  
286 intermingled to be indistinguishable with, information exempt under this subSection that is  
287 maintained by: (i) a covered entity or business associate; (ii) a health care facility or health care  
288 provider; or (iii) a program of a qualified service organization as defined by 42 U.S.C. 290dd-2.

289 (11) (i) An activity involving the processing of any personal information bearing on an  
290 individual's credit worthiness, credit standing, credit capacity, character, general reputation,  
291 personal characteristics, or mode of living by: (A) a consumer reporting agency, as defined in 15  
292 U.S.C. 1681a(f); (B) a furnisher of information, as set forth in 15 U.S.C. 1681s-2, that provides  
293 information for use in a consumer report, as defined in 15 U.S.C. 1681a(d); and (C) a user of a  
294 consumer report, as set forth in 15 U.S.C. 1681b.

295 (ii) Clause (i) of this paragraph shall apply only to the extent that: (A) the activity is  
296 regulated by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., as amended from time  
297 to time; and (B) the personal information is processed solely as authorized by the federal Fair  
298 Credit Reporting Act.

299 (12) Personal information processed in compliance with the federal Driver's Privacy  
300 Protection Act of 1994, 18 U.S.C. 2721 et seq. as amended from time to time, and implementing  
301 regulations.

302 (13) Personal information regulated by the federal Family Educational Rights and  
303 Privacy Act, 20 U.S.C. 1232g et seq. as amended from time to time, and its implementing  
304 regulations.

305 (14) Personal information processed in compliance with the federal Farm Credit Act, 12  
306 U.S.C. 2001 et seq. as amended from time to time, and its implementing regulations, 12 C.F.R.  
307 600 et seq.

308 (15) Personal information processed in compliance with the federal Gramm-Leach-Bliley  
309 Act, 15 U.S.C. 6801 et seq. as amended from time to time, and its implementing regulations.

310 (16) Personal information processed in compliance with chapter 175I of the General  
311 Laws.

312 (17) Personal information processed in relation to price, route or service, as such terms  
313 are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq. as amended from time to time,  
314 by an air carrier subject to said act, to the extent that this chapter is preempted by Section 41713  
315 of the Airline Deregulation Act.

316 (18) Personal information processed for purposes of chapter 176Q of the General Laws.

317 (g) Sections 8 through 11 and Section 13 of this chapter shall not apply to information  
318 that is processed: (1) in the course of an individual acting in a commercial context, to the extent  
319 that the information is collected and used within that context; (2) in the course of an individual  
320 acting as a job applicant to, an employee of, or an agent or independent contractor of a controller,  
321 processor, or third party, to the extent that the information is collected and used within the  
322 context of that role; (3) as the emergency contact information of an individual under paragraph



323 (2), provided that the information is used solely for emergency contact purposes; or (4) in order  
324 to administer benefits for another natural person relating to the individual under paragraph (2),  
325 provided that the information is used solely for the purposes of administering those benefits.

326 (h) The provisions of this chapter relating to individuals under 16 years of age shall only  
327 apply to the extent not in conflict with the federal Children's Online Privacy Protection Act, 15  
328 U.S.C. 6501 et seq., and its implementing regulations. Controllers and processors that comply  
329 with the Children's Online Privacy Protection Act and its implementing regulations shall be in  
330 compliance with any obligation to obtain parental consent under this chapter.

331 (i) This chapter shall also apply in full to an entity that voluntarily certifies to the  
332 Attorney General that it is in compliance with, and agrees to be bound by, this chapter; provided,  
333 however, that the entity processes the personal information of one or more individuals but does  
334 not meet the applicability criteria set forth in subsection (b) of this Section.

#### 335 Section 4. Conflicting Provisions

336 Wherever possible, law relating to individuals' personal information should be construed  
337 to harmonize with the provisions of this chapter, but in the event of a conflict between the  
338 provisions of other laws and the provisions of this chapter, the provisions that afford the greatest  
339 protection for the right of privacy for individuals shall control.

#### 340 Section 5. General Principles for Processing Personal Information

341 (a) Personal information shall be:

342 (1) Processed lawfully, fairly, and in a transparent manner in relation to the individual  
343 and in compliance with this chapter;

344 (2) Collected for specified, explicit and legitimate purposes and not further processed in a  
345 manner that is incompatible with those purposes;

346 (3) Processed in a manner that is adequate, relevant and limited to what is necessary in  
347 relation to the purposes for which it is processed;

348 (4) Maintained in a manner such that the information is accurate and, where necessary,  
349 kept up to date;

350 (5) Maintained in a form which permits identification of individuals for no longer than is  
351 necessary for the purposes for which the personal information is processed; and

352 (6) Processed in a manner that ensures that the information remains appropriately secure.

353 (b) A controller shall be responsible for, and capable of demonstrating compliance with,  
354 the above subSection (a), including by implementing procedures to comply with the subSection  
355 that are reasonable and appropriate taking into consideration:

356 (1) The size, scope, and type of the controller;

357 (2) The amount of resources available to the controller;

358 (3) The amount and nature of personal information processed by the controller, including,  
359 but not limited to, whether the personal information is sensitive information; and

360 (4) The need for the security and confidentiality of the personal information processed by  
361 the controller.

362 (c) A controller that is compliant with the regulations promulgated pursuant to chapter  
363 93H of the General Laws with respect to “personal information,” as that term is defined in

364 Section 1 of said chapter 93H, shall be in compliance with the principle set forth in paragraph (6)  
365 of subsection (a) of this Section with respect to such personal information.

366 Section 6. Lawful Bases For Processing Personal Information

367 (a) Processing shall be lawful and in compliance with this chapter only if and to the  
368 extent that at least 1 of the following applies:

369 (1) The individual has given consent to the processing of their personal information for  
370 one or more specific purposes;

371 (2) Processing is necessary for the performance of a contract to which the individual is  
372 party or in order to take steps at the request of the individual prior to entering into a contract;

373 (3) Processing is necessary for compliance with a legal obligation to which the controller  
374 is subject;

375 (4) Processing is necessary in order to protect the vital interests of the individual or of  
376 another natural person; provided, however, that the processing cannot be manifestly based on  
377 another legal basis and that the individual or other natural person is at risk or danger of death or  
378 serious physical injury; or

379 (5) Processing is necessary for the purposes of the legitimate interests pursued by the  
380 controller or by a third party, except where such interests are overridden by the individual's  
381 reasonable expectations of privacy or other legal rights.

382 (b) Processing pursuant to paragraph (5) of subsection (a) shall be consistent with the  
383 reasonable expectations of the individual based on the individual's relationship with the  
384 controller, and such processing shall be conspicuously disclosed to the individual in advance;

385 provided, however, that the controller shall also assess the following factors to determine  
386 whether there is a legitimate interest for the processing:

387 (1) The possible consequences and cognizable harms for the individual whose personal  
388 information would be processed;

389 (2) The amount and nature of personal information that would be processed;

390 (3) The need for the security and confidentiality of the personal information that would  
391 be processed;

392 (4) The context in which the personal information would be collected; and

393 (5) Whether the processing is necessary and proportionate in relation to the purposes, or  
394 whether the controller or third party can achieve their legitimate interests in another less intrusive  
395 way.

396 (c) A controller shall not rely on paragraph (5) of subsection (a) as a lawful basis for  
397 processing sensitive information unless the controller meets a heightened standard of proof,  
398 under which a controller shall conduct a documented risk assessment in accordance with Section  
399 21 of this chapter that shows that the legitimate interests pursued by the controller or by a third  
400 party substantially outweigh the individual's reasonable expectations of privacy or other legal  
401 rights. In particular, a controller shall not rely on paragraph (5) of subsection (a) to sell sensitive  
402 information that meets any of the subcategories set forth in paragraphs (1) through (5) in the  
403 definition of sensitive information in Section 2 of this chapter.

404 (d) A controller shall not sell the personal information of a child unless the controller has  
405 obtained the consent of the parent or guardian of the child.

406 (e) A controller shall not sell the personal information of a minor unless the controller has  
407 obtained the minor's consent.

408 (f) If a minor does not consent to the sale of the minor's personal information, a  
409 controller shall: (1) wait for not less than 12 months before making a subsequent request for the  
410 minor's consent to sell the minor's personal information; or (2) wait until the individual attains  
411 16 years of age, whichever occurs sooner.

## 412 Section 7. Right to Privacy Notice

413 (a) At or before the point of the collection of an individual's personal information,  
414 controllers shall provide the individual with a reasonably accessible, clear, and meaningful  
415 privacy notice that shall include:

416 (1) A clear and conspicuous description of: (i) whether the controller sells personal  
417 information to third parties or processes personal information for the purposes of targeted  
418 advertising; (ii) what categories of sensitive information, if any, the controller processes and for  
419 what purposes; (iii) an individual's rights pursuant to Sections 8 through 13 of this chapter; (iv)  
420 how and where individuals may request to exercise these rights, pursuant to Section 16 of this  
421 chapter; and (v) a link to the Attorney General's online mechanism through which the individual  
422 may contact the Attorney General to submit a complaint, pursuant to Section 25 of this chapter.

423 (2) The categories of personal information processed by the controller;

424 (3) The controller's purposes for processing the personal information;

425 (4) The categories of personal information that the controller sells to third parties,  
426 specifying the categories of sensitive information that the controller sells to third parties, if any;

427 (5) The categories of third parties, if any, to whom the controller sells personal  
428 information;

429 (6) A contact method, such as an email address, that the individual may use to contact the  
430 controller; and

431 (7) The length of time the controller intends to retain each category of personal  
432 information, or if that is not possible, the criteria used to determine such period, provided that a  
433 controller shall retain personal information for a duration consistent with paragraph (5) of  
434 subSection (a) of Section 5 of this chapter.

435 (b) A controller shall not collect additional categories of personal information or process  
436 personal information collected for additional purposes that are incompatible with the disclosed  
437 purposes for which the personal information was collected, without providing the individual with  
438 notice consistent with subSection (a) of this Section.

439 (c) An entity that, acting as a third party, controls the collection of an individual's  
440 personal information may satisfy its obligation under this Section by providing the required  
441 information prominently and conspicuously on the homepage of its Internet website; provided,  
442 however, that if an entity, acting as a third party, controls the collection of personal information  
443 about an individual on its premises, including in a vehicle, then the entity shall, at or before the  
444 point of collection, satisfy its obligation under subSection (a) of this Section by providing the  
445 required information in a clear and conspicuous manner at such location.

446 (d) Nothing in this Section shall require a controller to provide the information required  
447 in a manner that would disclose the controller's trade secrets.

448 (e) The categories of sensitive information required to be disclosed by a controller  
449 pursuant to this Section shall specifically include each applicable subcategory set forth in  
450 paragraphs (1) through (8) in the definition of sensitive information in Section 2 of this chapter.

#### 451 Section 8. The Right to Know and Access Personal Information

452 An individual shall have the right to request that a controller that collects personal  
453 information about the individual disclose to the individual:

454 (1) The specific pieces of personal information that the controller has collected about the  
455 individual; and

456 (2) The categories of sources from which the personal information has been collected.

#### 457 Section 9. Right to Data Portability

458 (a) In response to a verifiable request pursuant to Section 8 of this chapter, a controller  
459 shall disclose to the individual the information requested in the following manner:

460 (1) The controller shall provide to the individual the specific pieces of personal  
461 information that the controller has collected about the individual in a portable format that is  
462 easily understandable to the average individual and, to the extent technically feasible, in a readily  
463 usable format that allows the individual to transmit the information to another controller without  
464 hindrance. For the purposes of this subSection, “specific pieces of information” do not include  
465 any data generated to help ensure security and integrity.

466 (2) The controller shall also disclose the information specified in paragraph (2) of Section  
467 8 of this chapter, if so requested by the individual.

468 (3) The disclosure of the required information pursuant to paragraphs (1) and (2) of this  
469 subSection shall cover the 12 month period preceding the controller's receipt of the verifiable  
470 request; provided, however, that an individual may request that the controller disclose the  
471 required information beyond the 12 month period and the controller shall be required to provide  
472 such information unless doing so proves impossible or would constitute an undue burden for the  
473 controller. An individual's ability to request information beyond the 12 month period shall be  
474 clearly disclosed in a controller's privacy notice pursuant to clause (iii) of paragraph (1) of  
475 subSection (a) of Section 7 of this chapter.

476 (b) Nothing in this Section shall require a controller to provide the information requested  
477 in a manner that would disclose the controller's trade secrets.

#### 478 Section 10. Right to Delete Personal Information

479 (a) An individual shall have the right to request that a controller delete any personal  
480 information provided by or obtained about the individual.

481 (b) A controller that receives a verifiable request to delete the individual's personal  
482 information shall, pursuant to Section 17 of this chapter, delete the individual's personal  
483 information from its records, notify any processors to delete the individual's personal  
484 information from their records, and notify all third parties to whom the controller has sold the  
485 personal information to delete the individual's personal information unless doing so proves  
486 impossible or would constitute an undue burden for the controller.

487 (c) The controller may maintain a confidential record of deletion requests solely for the  
488 purpose of preventing the personal information of an individual who has submitted a deletion



489 request from being sold, for compliance with laws, or for other purposes solely to the extent  
490 permissible under this chapter.

491 (d) A controller, or a processor acting pursuant to its contract with the controller, shall  
492 not be required to comply with an individual's request to delete the individual's personal  
493 information if it is reasonably necessary for the controller or processor to maintain the  
494 individual's personal information in order to:

495 (1) Complete the transaction for which the personal information was collected, provide a  
496 good or service requested by the individual or reasonably anticipated by the individual within the  
497 context of a controller's ongoing relationship with the individual, or otherwise perform a contract  
498 between the controller and the individual;

499 (2) Enable solely internal uses that are reasonably aligned with the expectations of the  
500 individual based on the individual's relationship with the controller and compatible with the  
501 context in which the individual provided the information; or

502 (3) Comply with a legal obligation.

503 (e) The controller or processor shall retain personal information pursuant to subsection  
504 (d) solely for the applicable purposes under that subsection.

#### 505 Section 11. Right to Correct Personal Information

506 (a) An individual shall have the right to request that a controller correct inaccurate  
507 personal information concerning the individual, taking into account the nature of the personal  
508 information and the purposes of the processing of the personal information.

509 (b) A controller that receives a verifiable request to correct inaccurate personal  
510 information shall correct the inaccurate personal information as directed by the individual,  
511 pursuant to Section 17 of this chapter.

512 Section 12. Right to Opt Out of the Sale of Personal Information

513 (a) An individual shall have the right to opt out of the processing of the individual's  
514 personal information for the purposes of the sale of such personal information. This shall also be  
515 known as the right to opt out of the sale of personal information.

516 (b) A controller shall comply with a request to exercise the right to opt out of the sale of  
517 personal information as soon as reasonably possible, but not later than 30 days after receipt of  
518 the request. A controller that has received direction from an individual not to sell the individual's  
519 personal information shall be prohibited from selling the individual's personal information  
520 unless the individual subsequently provides consent for the sale of the individual's personal  
521 information pursuant to subsection (c).

522 (c) After complying with an individual's request to exercise the right to opt out of the sale  
523 of their personal information, a controller shall wait for not less than 12 months before  
524 requesting the individual's consent to sell the individual's personal information.

525 (d) A data broker shall not sell an individual's personal information unless the individual  
526 has received explicit notice and is provided an opportunity to exercise the right to opt out of the  
527 sale of their personal information.

528 (e) If a controller communicates to any entity authorized by the controller to collect  
529 personal information that an individual has requested to exercise the right to opt out of the sale of

530 their personal information, that entity shall thereafter only use that individual's personal  
531 information for purposes specified by the controller, or as otherwise permitted by this chapter,  
532 and shall be prohibited from:

533 (1) Selling the personal information; and

534 (2) Retaining, using, or disclosing that individual's personal information: (i) for any  
535 purpose other than for the specific purpose of performing the services offered to the controller;  
536 (ii) outside of the direct relationship between the entity and the controller; or (iii) for a  
537 commercial purpose other than providing the services to the controller.

538 (f) A controller that communicates an individual's opt-out request to an entity pursuant to  
539 subsection (e) shall not be liable under this chapter if the entity receiving the opt-out request  
540 violates the restrictions set forth in this chapter; provided, however, that at the time of  
541 communicating the opt-out request, the controller does not know or should not reasonably know  
542 that the entity intends to commit such a violation.

### 543 Section 13. Right to Limit Use and Disclosure of Sensitive Information

544 (a) An individual shall have the right to direct a controller that collects sensitive  
545 information about the individual to limit its use of the individual's sensitive information to that  
546 use which is necessary to perform the services or provide the goods reasonably expected by an  
547 average individual who requests those goods or services or to perform the following services:

548 (1) Short-term, transient use, including, but not limited to, nonpersonalized advertising  
549 shown as part of an individual's current interaction with the controller, provided that the  
550 individual's sensitive information is not disclosed to another third party and is not used to build a

551 profile about the individual or otherwise alter the individual's experience outside the current  
552 interaction with the controller;

553 (2) The performance of services on behalf of the controller, including maintaining or  
554 servicing accounts, providing customer service, processing or fulfilling orders and transactions,  
555 verifying customer information, processing payments, providing financing, providing analytic  
556 services, providing storage, or providing similar services on behalf of the controller;

557 (3) Undertaking activities to verify or maintain the quality or safety of a service or device  
558 that is owned, manufactured, manufactured for, or controlled by the controller, and to improve,  
559 upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or  
560 controlled by the controller; or

561 (4) Helping to ensure security and integrity, to the extent the use of the individual's  
562 personal information is reasonably necessary and proportionate for those purposes.

563 (b) A controller shall comply with a request to exercise the right in subsection (a) as soon  
564 as reasonably possible, but not later than 30 days after receipt of the request. A controller that  
565 has received direction from an individual not to use or disclose the individual's sensitive  
566 information, except as authorized under this Section, shall be prohibited from using or disclosing  
567 the sensitive information for any other purpose, unless the individual subsequently provides  
568 consent for the use or disclosure of the individual's sensitive information for additional purposes  
569 pursuant to subsection (c).

570 (c) For an individual who exercises the right in subsection (a), a controller shall wait for  
571 not less than 12 months before requesting the individual's consent to use and disclose the  
572 individual's sensitive information for additional purposes.

573 Section 14. Non-Discrimination Against Individuals' Good Faith Exercise of Privacy  
574 Rights

575 (a) A controller shall not discriminate against an individual for exercising, in good faith,  
576 any of the rights set forth in this chapter, including, but not limited to, by:

577 (1) Denying goods or services to the individual;

578 (2) Charging different prices or rates for goods or services, including through the use of  
579 discounts or other benefits or imposing penalties;

580 (3) Providing a different level of quality of goods or services to the individual;

581 (4) Suggesting that the individual will receive a different price or rate for goods or  
582 services or a different level of quality of goods or services; or

583 (5) Retaliating against a job applicant to, an employee of, or an agent or independent  
584 contractor of the controller for exercising their rights under this chapter.

585 (b) This Section shall not prohibit a controller from offering a different price, rate, level,  
586 quality, or selection of goods or services to an individual, including offering goods or services  
587 for no fee, if the offering is in connection with an individual's voluntary participation in a bona  
588 fide loyalty, rewards, premium features, discounts, or club card program.

589 Section 15. Exercising Privacy Rights

590 (a) An individual may exercise the rights set forth in Sections 8 through 13 of this chapter  
591 by submitting a request, at any time, to a controller specifying which rights the individual wishes  
592 to exercise.

593 (b) With respect to the processing of personal information of a child, the parent or legal  
594 guardian of the child may exercise the rights of this chapter on the child's behalf.

595 (c) With respect to the processing of personal information concerning an individual  
596 subject to guardianship, conservatorship, or other protective arrangement under article V or  
597 article 5A of chapter 190B of the General Laws, the guardian or the conservator of the individual  
598 may exercise the rights of this chapter on the individual's behalf.

599 (d) An individual may also designate an authorized agent to exercise, on behalf of that  
600 individual, the rights set forth in Sections 12 and 13 of this chapter; provided, however, that:

601 (1) Unless the individual has provided the authorized agent with power of attorney  
602 pursuant to Sections 5-501 through Sections 5-507 of article V of chapter 190B of the General  
603 Laws, a controller receiving a request from an authorized agent to exercise these rights may  
604 require the authorized agent to provide proof that the individual gave the agent permission to  
605 submit the request; provided, further, that if the controller has a reasonable basis to believe that  
606 the proof submitted by the agent is insufficient or invalid, the controller may also require the  
607 individual to do either of the following: (i) verify the individual's own identity directly with the  
608 controller; or (ii) directly confirm with the controller that the individual provided the authorized  
609 agent with permission to submit the request; and

610 (2) An authorized agent shall not use an individual's personal information, or any  
611 information collected from or about the individual, for any purposes other than to fulfill the  
612 individual's requests, for verification, or for fraud prevention and shall implement and maintain  
613 reasonable security procedures and practices to protect the individual's personal information.

614 Section 16. Disclosure of Methods for Exercising Privacy Rights

615 (a) A controller shall make available, and shall describe in a privacy notice pursuant to  
616 Section 7 of this chapter, not less than 2 designated methods for submitting a request to exercise  
617 the rights set forth in Sections 8 through 13 of this chapter. If a controller maintains an Internet  
618 website, the controller shall make its Internet website available as one such designated method  
619 for submitting a request to exercise the rights set forth in said Sections 8 through 13.

620 (b) A controller that sells individuals' personal information shall also provide a clear and  
621 conspicuous link on the controller's Internet homepages to an Internet web page that enables an  
622 individual, or an individual's authorized agent, to exercise their right to opt out of the sale of the  
623 individual's personal information.

624 (c) A controller that uses or discloses individuals' sensitive information for purposes  
625 other than those specified by Section 13 of this chapter shall also provide a clear and  
626 conspicuous link on the controller's Internet homepages that enables an individual, or an  
627 individual's authorized agent, to limit the use or disclosure of the individual's sensitive  
628 information to those purposes authorized under said Section 13.

629 (d) A controller that is subject to both subsections (b) and (c), in lieu of complying with  
630 both of those subsections, may utilize a single, clearly labeled link on the controller's Internet  
631 homepages, if that link easily allows an individual, or an individual's authorized agent, to  
632 exercise their right to opt out of the sale of the individual's personal information and to limit the  
633 use or disclosure of the individual's sensitive information.

634 (e) A controller shall:

635 (1) Ensure that all persons responsible for handling individuals' inquiries about the  
636 controller's privacy practices or the controller's compliance with this chapter are informed of: (i)

637 all requirements set forth under this chapter; and (ii) how to direct individuals to exercise their  
638 rights under Sections 8 through 13 of this chapter;

639 (2) Include a separate link to the applicable web pages required under subsections (b), (c),  
640 or (d) of this Section in any privacy notice that the controller is required to provide to individuals  
641 pursuant to Section 7 of this chapter;

642 (3) Use any personal information collected from the individual in connection with the  
643 submission of the individual's request to exercise any of the rights set forth in Sections 8 through  
644 13 of this chapter solely for the purposes of complying with the request;

645 (4) Use any personal information collected in connection with the controller's  
646 verification of the individual's request solely for the purposes of verification and shall not further  
647 disclose the personal information, retain it longer than necessary for purposes of verification, or  
648 use it for unrelated purposes; and

649 (5) Not require an individual to provide additional information beyond what is necessary  
650 to direct the controller to not sell the individual's personal information pursuant to Section 12 of  
651 this chapter, or to limit use or disclosure of the individual's sensitive information pursuant to  
652 Section 13 of this chapter.

### 653 Section 17. Responding to an Individual's Request

654 (a) Except as otherwise provided in this chapter, a controller shall comply with a request  
655 to exercise the rights set forth in Sections 8 through 11 of this chapter.

656 (b) A controller shall inform the individual of any action taken on a request to exercise  
657 any of the rights set forth in Sections 8 through 11 of this chapter without undue delay and in any



658 event within 45 days of receipt of the request; provided, however, that the period may be  
659 extended once by 45 additional days where reasonably necessary, taking into account the  
660 complexity and number of the requests. The controller shall notify the individual of any such  
661 extension within 45 days of receipt of the request, together with the reasons for the delay.

662 (c) A controller shall not be obligated to comply with a request to exercise the rights set  
663 forth in Sections 8 through 11 of this chapter if the request is not a verifiable request. In such a  
664 case, the controller shall notify the individual that it is unable to act on the request until it  
665 receives additional information reasonably necessary to verify that the request is being made by  
666 the individual or by another person who is entitled to exercise such rights on behalf of the  
667 individual pursuant to subsections (b) and (c) of Section 15 of this chapter.

668 (d) A verifiable request to exercise the rights set forth in Sections 8 through 11 of this  
669 chapter shall not extend to personal information about the individual that belongs to, or the  
670 controller maintains on behalf of, another natural person. A controller may rely on  
671 representations made in a verifiable request as to rights with respect to personal information and  
672 shall not be required to seek out other persons that may have or claim to have rights to personal  
673 information or to take any action under this chapter in the event of a dispute between or among  
674 persons claiming rights to personal information in the controller's possession.

675 (e) A request to exercise any of the rights in Sections 12 or 13 of this chapter shall not  
676 need to be a verifiable request. If a controller, however, has a good-faith, reasonable, and  
677 documented belief that the request is fraudulent, the controller may deny the request. The  
678 controller shall inform the requestor that it will not comply with the request and shall provide an  
679 explanation why it believes the request is fraudulent.

680 (f) When a controller, pursuant to subsection (b) of Section 23 of this chapter, is  
681 incapable of complying with an individual's verifiable request, the controller shall, if possible,  
682 notify the individual that it is not in a position to identify the individual. The individual, or a  
683 person entitled to exercise the rights of this chapter on behalf of the individual pursuant to  
684 subsections (b) and (c) of Section 15 of this chapter, may provide additional information to the  
685 controller enabling the individual's identification for the purposes of exercising their rights set  
686 forth in Sections 8 through 11 of this chapter.

687 (g) If a controller declines to take action regarding an individual's request, the controller  
688 shall notify the individual of the justification for declining to take action and provide the  
689 individual with instructions on how to submit a complaint pursuant to subsection (j) of this  
690 Section. Such notification shall occur without undue delay, but not later than 45 days after the  
691 initial receipt of the request or not later than 45 days after notifying the individual of the  
692 applicability of an extension pursuant to subsection (b) of this Section.

693 (h) A controller shall not be obligated to provide the information required by Section 9 of  
694 this chapter to the same individual more than twice in a 12 month period. Information provided  
695 in response to a request shall be provided by the controller to the individual free of charge.

696 (i) If requests from an individual, or from a person entitled to exercise the rights of this  
697 chapter on behalf of such individual pursuant to subsections (b) and (c) of Section 15 of this  
698 chapter, are manifestly unfounded or excessive, in particular because of their repetitive character,  
699 the controller may: (1) charge a reasonable fee to cover the administrative costs of complying  
700 with the request; or (2) refuse to act on the request. The controller shall bear the burden of  
701 demonstrating the manifestly unfounded or excessive nature of the request.

702 (j) When informing an individual of any action taken or not taken in response to a  
703 request, the controller shall provide the individual with a link to the Attorney General’s online  
704 mechanism through which the individual may contact the Attorney General to submit a  
705 complaint. The controller shall maintain records of all rejected requests for not less than 24  
706 months and shall compile and provide a copy of such records to the Attorney General upon the  
707 Attorney General’s request.

708 Section 18. No Waiver

709 Any provision of a contract or agreement of any kind that purports to waive or limit in  
710 any way individual rights under this chapter shall be deemed contrary to public policy and shall  
711 be void and unenforceable.

712 Section 19. Relationship Between Controllers and Processors

713 (a) A processor shall not be required to comply with a request pursuant to Sections 8  
714 through 13 of this chapter that the processor receives directly from an individual or from a  
715 person entitled to exercise such rights on behalf of the individual, to the extent that the processor  
716 has processed the individual’s personal information on behalf of the controller. A processor shall  
717 adhere to the instructions of the controller and shall assist the controller in meeting its  
718 obligations under this chapter. Such assistance shall include, but not be limited to, the following:

719 (1) Taking into account the nature of the processing and the information available to the  
720 processor, the processor shall assist the controller by taking appropriate technical and  
721 organizational measures, if possible, to fulfill the controller’s obligation to respond to  
722 individuals’ requests to exercise their rights pursuant to Sections 8 through 13 of this chapter,  
723 including by:

724 (i) Providing to the controller the individual's personal information, or correcting  
725 inaccurate personal information, in the processor's possession that the processor obtained as a  
726 result of providing services to the controller, or enabling the controller to do the same;

727 (ii) At the direction of the controller in response to a verifiable request pursuant to  
728 Section 10 of this chapter, deleting or enabling the controller to delete personal information  
729 about the individual processed by the processor on behalf of the controller; provided, however,  
730 that the processor shall notify any processors or third parties who may have accessed personal  
731 information from or through the processor to delete the individual's personal information, unless  
732 the information was accessed at the direction of the controller or unless doing so proves  
733 impossible or would constitute an undue burden; or

734 (iii) Not using sensitive information, after it has received instructions from the controller  
735 and to the extent it has actual knowledge that the personal information is sensitive information,  
736 for any purpose other than those authorized by Section 13 of this chapter; provided, however,  
737 that the processor shall only be required to limit its use of sensitive information received  
738 pursuant to a written contract with the controller in response to instructions from the controller  
739 and only with respect to its relationship with that controller;

740 (2) Taking into account the nature of the processing and the information available to the  
741 processor, the processor shall assist the controller in meeting the controller's obligations in  
742 relation to the security of processing the personal information and in relation to the notification  
743 of a breach of security of the system of the processor, pursuant to chapter 93H of the General  
744 Laws; and

745 (3) The processor shall provide information to the controller necessary to enable the  
746 controller to conduct and document any risk assessments required by Section 21 of this chapter.

747 (b) Notwithstanding the instructions of the controller, a processor shall ensure that each  
748 person processing personal information is subject to a duty of confidentiality with respect to the  
749 information.

750 (c) If a processor engages another entity to assist the processor in processing personal  
751 information on behalf of the controller, the processor shall provide the controller with an  
752 opportunity to object and the engagement shall be pursuant to a written contract, in accordance  
753 with subSection (e), that requires the entity to meet the obligations of the processor with respect  
754 to the personal information.

755 (d) The controller and the processor shall implement appropriate technical and  
756 organizational measures to ensure a level of security appropriate to the risk and establish a clear  
757 allocation of the responsibilities between them to implement such measures.

758 (e) A contract between a controller and a processor shall govern the processor's  
759 procedures with respect to processing individuals' personal information that the processor  
760 receives from or on behalf of the controller. The contract shall be binding on both parties and  
761 clearly set forth the processing instructions to which the processor is bound, including:

762 (1) The nature and purpose of the processing;

763 (2) The type of personal information subject to the processing;

764 (3) The duration of the processing;

765 (4) The rights and obligations of both parties;

766 (5) The requirements imposed by subsections (b) and (c); and

767 (6) The following requirements:

768 (i) At the controller's direction, the processor shall delete or return all personal  
769 information to the controller as requested at the end of the provision of services, unless retention  
770 of the personal information is required by law;

771 (ii) Upon the reasonable request of the controller, the processor shall make available to  
772 the controller all information in its possession necessary to demonstrate compliance with the  
773 obligations under this chapter;

774 (iii) The processor shall: (A) allow for, and cooperate with, reasonable audits and  
775 inspections by the controller or the controller's designated auditor; or (B) arrange for, with the  
776 controller's consent, a qualified and independent auditor to conduct, at least annually and at the  
777 processor's expense, an audit of the processor's policies and technical and organizational  
778 measures in support of the obligations under this chapter using an appropriate and accepted  
779 control standard or framework and audit procedure for such audits, provided that the processor  
780 shall disclose a report of the audit to the controller upon request; and

781 (iv) The processor shall be prohibited from: (A) selling the personal information; (B)  
782 retaining, using, or disclosing personal information other than for the purposes specified in the  
783 contract or as otherwise permitted by this chapter; (C) retaining, using, or disclosing personal  
784 information outside of the direct relationship between the processor and the controller; or (D)  
785 combining, for the purpose of targeted advertising, the personal information with the personal  
786 information that the processor receives from, or on behalf of, another entity or entities or that it  
787 collects from its own interaction with the individual.

788 (f) In no event may any contract relieve a controller or a processor from the liabilities  
789 imposed on it by this chapter.

790 (g) Determining whether an entity is acting as a controller or processor with respect to a  
791 specific processing of information is a fact-based determination that depends upon the context in  
792 which personal information is to be processed. A processor that continues to adhere to a  
793 controller's instructions with respect to a specific processing of personal information remains a  
794 processor. If a processor begins, alone or jointly with others, determining the purposes and  
795 means of the processing of personal information, it is a controller with respect to the processing.  
796 An entity that is not limited in its processing of personal information pursuant to a controller's  
797 instruction, or that fails to adhere to such instructions, is a controller and not a processor with  
798 respect to a specific processing.

799 Section 20. Data Broker Registration

800 (a) Not later than January 31 following each year in which a controller meets the  
801 definition of a data broker under this chapter, the controller shall register with the Attorney  
802 General pursuant to the requirements of this Section.

803 (b) When registering with the Attorney General, a data broker shall:

804 (1) Pay a registration fee of 200 dollars; and

805 (2) Provide the following information:

806 (i) The name of the data broker and its primary physical, email, and Internet website  
807 addresses;

808 (ii) Any privacy notice that a data broker discloses to individuals pursuant to Section 7 of  
809 this chapter;

810 (iii) How and where individuals may request to exercise the rights under Sections 12 and  
811 13 of this chapter;

812 (iv) Whether the data broker implements a purchaser credentialing process;

813 (v) Whether the data broker sells the personal information of individuals with whom the  
814 data broker does not have a direct relationship;

815 (vi) Whether the data broker sells the sensitive information of at least 10,000 individuals;

816 (vii) Whether the data broker processes the personal information of minors or children;

817 and

818 (viii) Any additional information or explanation the data broker may wish to provide.

#### 819 Section 21. Risk Assessments

820 (a) If a type of processing, taking into account the nature, scope, context and purposes of  
821 the processing and whether the processing involves new technologies, is likely to result in a high  
822 risk of harm to the individual, the controller shall, prior to the processing, carry out a risk  
823 assessment of the impact of the envisioned processing operations on the protection of personal  
824 information. A single assessment may address a set of similar processing operations that present  
825 similar high risks.

826 (b) In particular, a controller shall conduct a risk assessment in the case of:

827 (1) The processing of sensitive information;



828 (2) The sale of personal information; or

829 (3) A systematic and extensive evaluation of personal aspects relating to individuals that  
830 is based on automated processing, on which decisions are based that present a reasonably  
831 foreseeable risk of: (i) unfair or deceptive treatment of, or unlawful disparate impact on, certain  
832 individuals; (ii) financial, physical, or reputational harm to individuals; (iii) a physical or other  
833 intrusion upon the solitude or seclusion, or the private affairs or concerns, of individuals, where  
834 such intrusion would be offensive to a reasonable person; or (iv) other substantial cognizable  
835 harms to individuals.

836 (c) The assessment shall contain at a minimum:

837 (1) A systematic description of the envisioned processing operations and the purposes of  
838 the processing, including, where applicable, the legitimate interest pursued by the controller or  
839 third party;

840 (2) An assessment of the necessity of the processing operations in relation to the  
841 purposes, taking into account whether the controller or third party can achieve their legitimate  
842 interests in another less intrusive way;

843 (3) An assessment of the proportionality of the processing operations in relation to the  
844 purposes, taking into account the amount and nature of the personal information to be processed;

845 (4) An assessment of the risks to individuals;

846 (5) The measures envisioned to address the risks, including safeguards such as de-  
847 identification, security measures and mechanisms to ensure the protection of personal

848 information and to demonstrate compliance with this chapter taking into account the individuals'  
849 reasonable expectations of privacy or other legal rights; and

850 (6) A description of: (i) the context of the processing; (ii) the relationship between the  
851 controller and the individual whose personal information would be processed; and (iii) whether  
852 the controller is processing an individual's personal information in ways in which the individual  
853 would reasonably expect.

854 (d) Subsections (a) through (c) shall not apply to processing pursuant to paragraph (3) of  
855 Section 6 of this chapter that has a legal basis in any federal or state law to which the controller  
856 is subject; provided, however, that the law regulates the specific processing operation or set of  
857 operations in question and the controller has already carried out a risk assessment that has  
858 reasonably comparable scope and effect for the purpose of compliance with that law.

859 (e) Where necessary, the controller shall carry out a review to assess if processing is  
860 performed in accordance with the risk assessment at least when there is a change of the risk  
861 represented by processing operations.

862 (f) A controller shall implement procedures to comply with this Section that are  
863 reasonable and appropriate taking into consideration:

864 (1) The size, scope, and type of the controller;

865 (2) The amount of resources available to the controller;

866 (3) The amount and nature of personal information processed by the controller, including,  
867 but not limited to, whether the personal information is sensitive information; and

868 (4) The need for the security and confidentiality of the personal information processed by  
869 the controller.

870 (g) The Attorney General may require, pursuant to a civil investigative demand, that a  
871 controller disclose any risk assessment that is relevant to an investigation conducted by the  
872 Attorney General. The controller shall accordingly make the risk assessment available to the  
873 Attorney General, and the Attorney General may evaluate the risk assessment for compliance  
874 with the responsibilities in this chapter. Risk assessments shall be confidential and exempt from  
875 public inspection and copying under chapter 66 of the General Laws. The disclosure of a risk  
876 assessment pursuant to a civil investigative demand from the Attorney General shall not  
877 constitute a waiver of attorney-client privilege or work product protection with respect to the  
878 assessment and any information contained in the assessment.

879 (h) Risk assessments shall apply to processing activities created or generated after this  
880 chapter is enacted and shall not be retroactive.

#### 881 Section 22. Processing That Unlawfully Discriminates

882 (a) A controller that processes personal information in a manner that violates chapter  
883 151B of the General Laws or any other state or federal law prohibiting unlawful discrimination  
884 against individuals shall also be in violation of this chapter.

885 (b) Nothing in this Section shall be construed to limit controllers from processing  
886 personal information for legitimate testing to prevent unlawful discrimination or otherwise  
887 determine the extent or effectiveness of the controller's compliance with this Section.

#### 888 Section 23. De-identified Information

889 (a) A controller that possesses de-identified information shall:

890 (1) Take reasonable technical and organizational measures to ensure that the information  
891 cannot be associated with an identified or identifiable individual or household;

892 (2) Not attempt to re-identify the information, provided that the controller may attempt to  
893 re-identify the information solely for the purpose of determining whether its de-identification  
894 procedures satisfy the requirements of this subsection; and

895 (3) Contractually require any recipients of the information to comply with all the  
896 requirements of this subsection.

897 (b) This chapter shall not be construed to require a controller or processor to do any of  
898 the following solely for the purpose of complying with this chapter:

899 (1) Maintain information in an identifiable, linkable, or associable form, or collect,  
900 obtain, retain, or access any information or technology, in order to be capable of linking or  
901 associating a verifiable request with personal information; or

902 (2) Reidentify or otherwise link de-identified information, provided that the controller  
903 provides applicable notice to the individual pursuant to subsection (f) of Section 17 of this  
904 chapter.

905 Section 24. Limitations.

906 (a) The obligations imposed on controllers or processors under this chapter shall not  
907 restrict a controller's or a processor's ability to:

908 (1) Comply with federal, state, or local laws, rules or regulations;

909 (2) Comply with a civil, criminal, or regulatory inquiry, subpoena, or summons by  
910 federal, state, local, or other governmental authorities;

911 (3) Cooperate with law enforcement agencies concerning conduct or activity that the  
912 controller or processor reasonably and in good faith believes may violate federal, state, or local  
913 laws, rules, or regulations;

914 (4) Investigate, establish, exercise, prepare for, or defend legal claims;

915 (5) Take immediate steps to protect the security or protection of an individual or another  
916 natural person, if that individual or other natural person is at risk or danger of death or serious  
917 physical injury; or

918 (6) Assist another controller, processor, or third party with any of the obligations under  
919 this subsection.

920 (b) The obligations imposed on controllers or processors under Sections 8 through 13 of  
921 this chapter shall not restrict a controller or processor's ability to retain or process information  
922 for the following purposes, provided that the use of the individual's personal information is  
923 reasonably necessary and proportionate for the purposes:

924 (1) Helping to ensure security and integrity;

925 (2) Debugging to identify and repair errors that impair existing intended functionality;

926 (3) Fulfilling the terms of a written warranty or product recall conducted in accordance  
927 with federal law;

928 (4) Engaging in public or peer-reviewed scientific, historical, or statistical research in the  
929 public interest that conforms or adheres to all other applicable ethics and privacy laws; provided,  
930 however, that:

931 (i) Such research is approved, monitored, and governed by an institutional review board,  
932 human subjects research ethics review board, or a similar independent oversight entity that  
933 determines: (A) if the research is likely to provide substantial benefits that do not exclusively  
934 accrue to the controller; (B) the expected benefits of the research outweigh the privacy risks; and  
935 (C) if the controller has implemented reasonable safeguards to mitigate privacy risks associated  
936 with research, including any risks associated with reidentification; or

937 (ii) A controller's deletion of the personal information pursuant to a request under  
938 Section 10 of this chapter is likely to render impossible or seriously impair the ability to  
939 complete such research.

940 (d) Obligations imposed on controllers or processors under this chapter shall not:

941 (1) Apply to the processing of personal information by a natural person in the course of a  
942 purely personal or household activity;

943 (2) Apply where compliance by the controller or processor would violate an evidentiary  
944 privilege under the laws of the Commonwealth or be construed to prevent a controller or  
945 processor from providing personal information concerning an individual to a person covered by  
946 an evidentiary privilege under the laws of the Commonwealth as part of a privileged  
947 communication;

948 (3) Adversely affect the right of an individual or any other person to exercise free speech,  
949 pursuant to the First Amendment to the United States Constitution, or to exercise another right  
950 provided for by law; or

951 (4) Apply to an entity's publication of entity-based member or employee contact  
952 information where such publication is intended to allow members of the public to contact such  
953 member or employee in the ordinary course of the entity's operations.

954 (e) Personal information that is processed by a controller pursuant to an exemption under  
955 subsections (a) through (d) of this Section:

956 (1) Shall not be processed for any purpose other than those expressly listed in subsections  
957 (a) through (d), unless otherwise allowed by this chapter; and

958 (2) Notwithstanding anything in this Section to the contrary, shall be processed in  
959 accordance with Section 5 of this chapter and subject to reasonable administrative, technical, and  
960 physical measures to reduce reasonably foreseeable risks of harm to individuals.

961 (f) If a controller processes personal information pursuant to an exemption in subsections  
962 (a) through (d) of this Section, the controller bears the burden of demonstrating that such  
963 processing qualifies for the exemption and complies with the requirements in subsection (e).

964 (g) A controller or processor that discloses personal information to a processor or third  
965 party in compliance with the requirements of this chapter is not in violation of this chapter if the  
966 recipient processes such personal information in violation of this chapter; provided, however,  
967 that at the time of disclosing the personal information, the disclosing controller or processor did  
968 not know or should not reasonably have known that the recipient intended to commit a violation.

969 (h) A processor or third party receiving personal information from a controller or  
970 processor in compliance with the requirements of this chapter is not in violation of this chapter if  
971 the controller or processor from which it receives the personal information fails to comply with  
972 applicable obligations under this chapter; provided, however, that the processor or third party  
973 shall be liable for its own violations of this chapter.

974 (i) If an individual has already consented to a controller's use, disclosure, or sale of their  
975 personal information to produce a physical item, such as a school yearbook, Sections 10 through  
976 13 of this chapter shall not apply to the controller's use, disclosure, or sale of the particular  
977 pieces of the individual's personal information for the production of that physical item; provided,  
978 however, that:

979 (1) The controller has incurred significant expense in reliance on the individual's consent;

980 (2) Compliance with the individual's request to exercise any of the rights in Sections 10  
981 through 13 would not be commercially reasonable; and

982 (3) The controller complies with the individual's request as soon as it is commercially  
983 reasonable to do so.

#### 984 Section 25. Powers of the Attorney General

985 (a) Whenever the Attorney General of the Commonwealth has reasonable cause to  
986 believe that an entity has engaged in, is engaging in, or is about to engage in a violation of this  
987 chapter, the Attorney General may issue a civil investigative demand. The provisions of Section  
988 6 of chapter 93A of the General Laws shall apply mutatis mutandis to civil investigative  
989 demands issued under this chapter.



990 (b) The Attorney General shall have the authority to enforce the provisions of this  
991 chapter. A violation of this chapter shall not serve as the basis for or be subject to a private right  
992 of action under this chapter. Nothing in this chapter shall be construed as creating a new private  
993 right of action or serving as the basis for a private right of action that would not otherwise have  
994 had a basis under any other law but for the enactment of this chapter. This chapter neither  
995 relieves any party from any duties or obligations imposed, nor alters any independent rights that  
996 individuals have, under chapter 93A of the General Laws, other state or federal laws, the  
997 Massachusetts Constitution, or the United States Constitution.

998 (c) Prior to initiating any civil action under this chapter, the Attorney General shall  
999 provide an entity written notice identifying the specific provisions of this chapter that the  
1000 Attorney General alleges have been or are being violated.

1001 (d) (1) The entity shall have a period of 30 days in which to cure a violation after being  
1002 provided notice by the Attorney General. If within that time period the entity cures the noticed  
1003 violation and provides the Attorney General an express written statement that the alleged  
1004 violations have been cured and that no further violations shall occur, no action shall be initiated  
1005 against the entity.

1006 (2) Paragraph (1) shall not apply when:

1007 (i) The court has previously issued a temporary restraining order, preliminary injunction,  
1008 or permanent injunction or assessed civil penalties against the entity for a violation of this  
1009 chapter;

1010 (ii) The Attorney General and the entity have previously reached a settlement relating to  
1011 this chapter that includes an admission by the entity that it has violated this chapter, not  
1012 including any express written statement provided pursuant to paragraph (1);

1013 (iii) The Attorney General has clear and convincing evidence that the entity willfully and  
1014 wantonly violated this chapter;

1015 (iv) The violation is a data broker's failure to register pursuant to Section 20 of this  
1016 chapter; or

1017 (v) The violation occurs more than twenty four months after the effective date of this  
1018 Section and the violating entity: (A) as of January 1 of the calendar year, had annual global gross  
1019 revenues in excess of 1,000,000,000 dollars in the preceding calendar year; and (B) determines  
1020 the purposes and means of processing of the personal information of not less than 100,000  
1021 individuals.

1022 (3) In its notice pursuant to subsection (c), the Attorney General shall specify the length,  
1023 if any, of the period in which the entity can cure the noticed violation.

1024 (e) If an entity continues to violate this chapter following the cure period in subsection  
1025 (d), breaches an express written statement provided to the Attorney General under that  
1026 subsection, or is not eligible for a cure period pursuant to that subsection, the Attorney General  
1027 may initiate a civil action against the entity in the name of the Commonwealth or as *parens*  
1028 *patriae* on behalf of individuals. The Attorney General may seek a temporary restraining order,  
1029 preliminary injunction, or permanent injunction to restrain any violations of this chapter and may  
1030 seek civil penalties of up to 7,500 dollars for each violation under this chapter, not including  
1031 violations of Section 20 of this chapter.

1032 (f) The superior court shall have jurisdiction of actions brought under this Section. Such  
1033 actions may be brought in any county where a defendant resides or has its principal place of  
1034 business or in which the violation occurred in whole or in part, or, with the consent of a  
1035 defendant, in the superior court for Suffolk County.

1036 (g) In determining the overall amount of civil penalties to seek or assess against an entity,  
1037 the Attorney General or the court shall include, but not be limited to, the following in its  
1038 consideration:

1039 (1) The size, scope, and type of the entity;

1040 (2) The amount of resources available to the entity;

1041 (3) The amount and nature of personal information processed by the entity;

1042 (4) The number of violations;

1043 (5) The number of violations affecting minors or children;

1044 (6) The nature and severity of the violation;

1045 (7) The risks caused by the violation;

1046 (8) Whether the entity's violation was not an isolated instance but instead part of a  
1047 pattern of violations and noncompliance with this chapter;

1048 (9) Whether the entity is a data broker that did not register pursuant to Section 20 of this  
1049 chapter;

1050 (10) Whether the violation was willful and not the result of error;

- 1051 (11) The length of time over which the violation occurred;
- 1052 (12) The precautions taken by the entity to prevent a violation;
- 1053 (13) The good faith cooperation of the entity with any investigations conducted by the  
1054 Attorney General pursuant to this Section;
- 1055 (14) Efforts undertaken by the entity to cure the violation; and
- 1056 (15) The entity's past violations of information privacy rules, regulations, codes,  
1057 ordinances, and laws in other jurisdictions.

1058 (h) A data broker that fails to register as required by Section 20 of this chapter may be  
1059 subject to injunction and liable for civil penalties, fees, and costs in a civil action brought on  
1060 behalf of the Commonwealth by the Attorney General as follows:

1061 (1) A civil penalty of up to 500 dollars for each day, not to exceed a total of 100,000  
1062 dollars for each year, the data broker fails to register as required by this Section; and

1063 (2) Fees equal to the fees that were due during the period the data broker failed to  
1064 register.

1065 (i) Any entity that violates the terms of an injunction or other order issued under this  
1066 Section shall forfeit and pay a civil penalty of up to 10,000 dollars for each violation. For the  
1067 purposes of this Section, the court issuing such an injunction or order shall retain jurisdiction,  
1068 and the cause shall be continued, and in such case the Attorney General acting in the name of the  
1069 Commonwealth may petition for recovery of such civil penalty.

1070 (j) The Attorney General may recover reasonable expenses incurred in investigating and  
1071 preparing the case, including attorney fees, in any action initiated under this chapter.

1072 (k) If two or more entities are involved in the same processing that violates this chapter,  
1073 the liability shall be allocated among the parties according to principles of comparative fault.

1074 (l) Notwithstanding any general or special law to the contrary, the court may require that  
1075 the amount of a civil penalty imposed pursuant to this Section exceeds the economic benefit  
1076 realized by an entity for noncompliance.

1077 (m) If a series of steps or transactions were component parts of a single transaction  
1078 intended to avoid the reach of this chapter, the Attorney General and the court shall disregard the  
1079 intermediate steps or transactions and consider everything one transaction for purposes of  
1080 effectuating the purposes of this chapter.

1081 (n) Not later than 30 days after the end of each calendar year, the Attorney General shall  
1082 publish a public, easily accessible report that provides, for that calendar year, the following  
1083 information:

1084 (1) Anonymized examples of alleged violations that have been cured by an entity  
1085 pursuant to subsection (d); provided, however, that these examples shall protect the  
1086 confidentiality of the entity;

1087 (2) The number of written notices issued pursuant to subsection (c);

1088 (3) The number of entities that received written notices issued pursuant to subsection (c);

1089 and

1090 (4) The categories of violations of this chapter and the number of violations per category.

1091 (o) The Attorney General shall receive and may investigate sworn complaints from an  
1092 individual or other natural person that an entity has engaged in, is engaging in, or is about to  
1093 engage in any violation of this chapter. The Attorney General shall notify the individual or other  
1094 natural person who made the complaint of the action, if any, the Attorney General has taken or  
1095 plans to take on the complaint, together with the reasons for that action or nonaction.

1096 (p) The Attorney General shall maintain the following Internet web pages: (1) a web page  
1097 that includes an online mechanism through which any individual or other natural person may  
1098 contact the Attorney General to submit a sworn complaint; (2) a web page that enables data  
1099 brokers to register pursuant to Section 20 of this chapter; and (3) a web page that makes publicly  
1100 accessible the information provided by data brokers pursuant to Section 20 of this chapter.

1101 (q) The Attorney General shall promote public awareness and understanding of the risks,  
1102 rules, responsibilities, safeguards, and rights in relation to the processing of personal  
1103 information, including the rights of individuals under the age of 16 with respect to their own  
1104 information. The Attorney General shall provide guidance to individuals regarding what to do if  
1105 they believe their rights under this chapter have been violated.

1106 (r) The Attorney General shall create and make publicly accessible the following  
1107 templates: (1) a template privacy policy that meets the requirements of Section 7 of this chapter;  
1108 (2) a template contract between a controller and a processor that meets the requirements of  
1109 Section 19 of this chapter; and (3) a template risk assessment that meets the requirements of  
1110 Section 21 of this chapter.

1111 (s) The Attorney General shall have the power to determine, pursuant to Section 27 of  
1112 this chapter, whether the provisions of a personal information privacy law in another jurisdiction  
1113 are equally or more protective of personal information than the provisions in this chapter.

1114 (t) The Attorney General shall establish a mechanism pursuant to which an entity that  
1115 processes the personal information of one or more individuals but does not meet the applicability  
1116 criteria set forth in subsection (b) of Section 3 of this chapter may voluntarily certify that it is in  
1117 compliance with, and agrees to be bound by, this chapter. The Attorney General shall make a list  
1118 of those entities available to the public.

1119 (u) The Attorney General shall adopt regulations for the purposes of carrying out this  
1120 chapter, including, but not limited to, the following areas:

1121 (1) Supplementing any of the definitions used in this chapter or adding in new definitions  
1122 for terms that are used but not otherwise defined in this chapter, in order to address changes in  
1123 technology, data collection, obstacles to implementation, and privacy concerns; and

1124 (2) Ensuring that the notices and information that controllers are required to provide  
1125 pursuant to Section 7 of this chapter are provided in a manner that may be easily understood by  
1126 the average individual, are accessible to individuals with disabilities, and are available in the  
1127 language primarily used to interact with the individual.

1128 (v) The Attorney General shall conduct research and monitor relevant developments  
1129 relating to the protection of personal information, the development of information and  
1130 communication technologies and commercial practices, and the enactment and implementation  
1131 of privacy laws in other states, territories, and countries or by the federal government. Specific

1132 topics for research by the Attorney General shall include, but are not limited to, the following  
1133 areas:

1134 (1) The available best methods for an individual to exercise the rights set forth in  
1135 Sections 8 through 13 of this chapter, including: (i) the development of technology, such as a  
1136 browser setting, browser extension, or global device setting, indicating an individual's  
1137 affirmative, freely given, and unambiguous choice to opt out of the sale of the individual's  
1138 personal information or to limit the use or disclosure of the individual's sensitive information;  
1139 (ii) the development of technology that enables an individual to opt out of the sale of the  
1140 individual's personal information by all data brokers that have registered pursuant to Section 20  
1141 of this chapter; and (iii) ways for entities to conspicuously and clearly disclose how to exercise  
1142 the rights set forth in Sections 8 through 13;

1143 (2) Access and opt-out rights with respect to controllers' use of automated decision-  
1144 making technology;

1145 (3) Eye-tracking technology and targeted advertising based on information collected  
1146 through eye-tracking technology;

1147 (4) Financial incentive programs offered by controllers for the processing of personal  
1148 information;

1149 (5) The targeting of advertising based on a profile of an individual created by an  
1150 individual's activity over time with regard to an entity's own businesses, distinctly-branded  
1151 websites, applications, or services;



1152 (6) The data broker industry, including data brokers that have registered pursuant to  
1153 Section 20 of this chapter;

1154 (7) The effectiveness of allowing an individual to designate an authorized agent to  
1155 exercise a right on their behalf pursuant to subsection (d) of Section 15 of this chapter; and

1156 (8) Whether to change or eliminate the cure period established in subsection (d) of  
1157 Section 25 of this chapter.

1158 (w) At least once per calendar year, the Attorney General shall provide a full written  
1159 report to the Legislature's Joint Committee on Advanced Information Technology, the Internet  
1160 and Cybersecurity. The report shall summarize the Attorney General's research and any  
1161 recommendations with respect to privacy-related legislation. The first such report provided by  
1162 the Attorney General shall be submitted within 12 months of the effective date of this subsection  
1163 and shall include a summary of the Attorney General's research and recommendations pursuant  
1164 to paragraphs (1) through (5) of subsection (v).

1165 (x) The monetary amounts referred to in this chapter shall be indexed for inflation by the  
1166 Attorney General, who, not later than December 31 of each even numbered year, shall calculate  
1167 and publish such indexed amounts, using the federal consumer price index for the Boston  
1168 statistical area and rounding to the nearest dollar.

1169 Section 26. Massachusetts Privacy Fund.

1170 (a) There shall be established upon the books of the Commonwealth a separate special  
1171 fund to be known as the Massachusetts Privacy Fund.

1172 (b) All civil penalties, expenses, attorney fees, and registration fees collected pursuant to  
1173 Sections 20 and 25 of this chapter shall be paid into the state treasury and credited to the  
1174 Massachusetts Privacy Fund. Interest earned on moneys in the Fund shall remain in the Fund and  
1175 be credited to it. Any moneys remaining in the Fund, including interest thereon, at the end of  
1176 each fiscal year shall not revert to the general fund but shall remain in the Fund.

1177 (c) The Attorney General shall have discretion to allocate the proceeds of any settlement  
1178 of a civil action pursuant to this chapter to: (1) the Massachusetts Privacy Fund; (2) the general  
1179 fund; or (3) where possible, directly to individuals impacted by the violation of the chapter.

1180 (d) Moneys in the Massachusetts Privacy Fund shall be used to support the work of the  
1181 Attorney General pursuant to Section 25 of this chapter. Moneys in the Massachusetts Privacy  
1182 Fund shall be subject to appropriation and shall not be used to supplant general fund  
1183 appropriations to the Attorney General.

#### 1184 Section 27. Reciprocity and Interoperability

1185 (a) A controller or processor shall be in compliance with provisions of this chapter if: (1)  
1186 it complies with comparable provisions of a personal information privacy law in another  
1187 jurisdiction; (2) the controller or processor applies the provisions of that law to its processing  
1188 activities concerning individuals; and (3) the Attorney General determines that the provisions of  
1189 that law in the other jurisdiction are equally or more protective of personal information than the  
1190 provisions of this chapter.

1191 (b) The Attorney General may charge a fee to a controller or processor that asserts  
1192 compliance with a comparable law under subSection (a); provided, however, that the fee shall

1193 reflect costs reasonably expected to be incurred by the Attorney General to determine whether  
1194 the provisions of said law are equally or more protective than the provisions of this chapter.

1195 Section 28. Delayed Implementation for Nonprofits and Institutions of Higher Education

1196 This chapter shall not apply to institutions of higher education or nonprofit organizations  
1197 until 24 months after the effective date of this Section.

1198 Section 29. Severability

1199 (a) The provisions of this chapter are severable. If any provision of this chapter, or the  
1200 application of any provision of this chapter, is held invalid, the remaining provisions, or  
1201 applications of provisions, shall remain in full force and not be affected.

1202 (b) If a court were to find in a final, unreviewable judgment that the exclusion of one or  
1203 more entities or activities from the applicability of this chapter renders the chapter  
1204 unconstitutional, those exceptions shall be rendered null and invalid and the exemption shall not  
1205 continue.

1206 SECTION 2. Chapter 93H of the General Laws is hereby amended by inserting after  
1207 Section 6 of said chapter the following Section:

1208 Section 7. Private Right of Action and Safe Harbor

1209 (a) For the purposes of this Section, the term “personal information” shall have the same  
1210 meaning as defined in Section 1 of this chapter, except that for the purposes of subsections (c)  
1211 and (d) of this Section, the term “personal information” shall have the same meaning as in  
1212 Section 2 of chapter 93M of the General Laws.

1213 (b) For the purposes of this Section, the following terms shall have the same meanings as  
1214 such terms are defined in Section 2 of chapter 93M of the General Laws: “controller”; “data  
1215 broker,” “individual”; “process”; and “sell.”

1216 (c) This Section shall apply to a controller that:

1217 (1) Conducts business in the Commonwealth or is not physically established in the  
1218 Commonwealth but processes personal information where such processing activities are related  
1219 to: (i) the offering of goods or services that are targeted to individuals; or (ii) the monitoring of  
1220 behavior of individuals where such behavior takes place in the Commonwealth; and

1221 (2) Meets 1 of the following additional thresholds:

1222 (i) The controller, as of January 1 of the calendar year, had annual global gross revenues  
1223 in excess of 25,000,000 dollars in the preceding calendar year;

1224 (ii) The controller determines the purposes and means of processing of the personal  
1225 information of not less than 100,000 individuals; or

1226 (iii) The controller is a data broker.

1227 This Section shall also apply to an entity that is an affiliate of and shares common  
1228 branding with such a controller, with respect to the personal information processed by the  
1229 affiliate on behalf of the controller.

1230 (d) This Section shall not apply to controllers and information that are fully exempt from  
1231 the provisions of chapter 93M of the General Laws pursuant to Section 3 of that chapter;  
1232 provided, however, that this Section shall apply to an activity involving the processing of any  
1233 personal information bearing on an individual’s credit worthiness, credit standing, credit

1234 capacity, character, general reputation, personal characteristics, or mode of living by: (A) a  
1235 consumer reporting agency, as defined in 15 U.S.C. 1681a(f); (B) a furnisher of information, as  
1236 set forth in 15 U.S.C. 1681s-2, that provides information for use in a consumer report, as defined  
1237 in 15 U.S.C. 1681a(d); and (C) a user of a consumer report, as set forth in 15 U.S.C. 1681b.

1238 (e) Any individual whose personal information is subject to a breach of security, as  
1239 defined in Section 1 of this chapter, as a result of a controller's failure to implement and maintain  
1240 reasonable cybersecurity controls may institute a civil action for any of the following:

1241 (1) Damages from the controller in an amount up to 500 dollars per individual per  
1242 incident or actual damages, whichever is greater;

1243 (2) Injunctive or declaratory relief;

1244 (3) Any other relief the court deems proper.

1245 (f) In assessing the amount of statutory damages against the controller, the court shall  
1246 include, but not be limited to, the following in its consideration:

1247 (1) The size, scope, and type of the entity;

1248 (2) The amount of resources available to the entity;

1249 (3) The amount and nature of personal information processed by the entity;

1250 (4) The number of violations;

1251 (5) The number of violations affecting minors or children;

1252 (6) The nature and severity of the violation;

- 1253 (7) The risks caused by the violation;
- 1254 (8) Whether the entity’s violation was not an isolated instance but instead part of a  
1255 pattern of violations and noncompliance with this chapter;
- 1256 (9) Whether the entity is a data broker that did not register pursuant to Section 20 of  
1257 chapter 93M of the General Laws;
- 1258 (10) Whether the violation was willful and not the result of error;
- 1259 (11) The length of time over which the violation occurred;
- 1260 (12) The precautions taken by the entity to prevent a violation;
- 1261 (13) The good faith cooperation of the entity;
- 1262 (14) Efforts undertaken by the entity to cure the violation; and
- 1263 (15) The entity’s past violations of rules, regulations, codes, ordinances, and laws in other  
1264 jurisdictions regarding breaches of security.
- 1265 (g) In any cause of action founded in tort that is brought pursuant to this Section and that  
1266 alleges that the controller’s failure to implement reasonable cybersecurity controls resulted in a  
1267 breach of security concerning personal information, the court shall not assess punitive damages  
1268 against a controller if such controller:
- 1269 (1) Created, maintained and complied with a written cybersecurity program that contains  
1270 administrative, technical and physical safeguards for the protection of personal information and  
1271 that conforms to an industry recognized cybersecurity framework, as described in subsection (i);  
1272 and

1273 (2) Designed its cybersecurity program in accordance with the provisions of subsections  
1274 (k) and (l).

1275 (h) Subsection (g) shall not apply if the controller's failure to implement reasonable  
1276 cybersecurity controls was the result of gross negligence or willful or wanton conduct.

1277 (i) A controller's cybersecurity program, as described in subsection (g), shall conform to  
1278 an industry recognized cybersecurity framework if:

1279 (1) The cybersecurity program conforms to the current version of or any combination of  
1280 the current versions of:

1281 (i) The "Framework for Improving Critical Infrastructure Cybersecurity" published by  
1282 the National Institute of Standards and Technology;

1283 (ii) The National Institute of Standards and Technology's special publication 800-171;

1284 (iii) The National Institute of Standards and Technology's special publications 800-53  
1285 and 800-53a;

1286 (iv) The Federal Risk and Authorization Management Program's "FedRAMP Security  
1287 Assessment Framework";

1288 (v) The Center for Internet Security's "Center for Internet Security Critical Security  
1289 Controls for Effective Cyber Defense"; or

1290 (vi) The "ISO/IEC 27000-series" information security standards published by the  
1291 International Organization for Standardization and the International Electrotechnical  
1292 Commission; or

1293 (2) The cybersecurity program complies with the current version of the “Payment Card  
1294 Industry Data Security Standard” and the current version of another applicable industry  
1295 recognized cybersecurity framework described in paragraph (1) of this subsection.

1296 (j) When a revision to a document listed in paragraph (1) or (2) of subsection (i) is  
1297 published, a controller whose cybersecurity program conforms to a prior version of that  
1298 document shall be said to conform to the current version of that document if the controller  
1299 conforms to such revision not later than six months after the publication date of the revision.

1300 (k) For the purposes of complying with this Section, a controller’s cybersecurity program  
1301 shall be implemented in accordance with the regulations adopted pursuant to chapter 93H of the  
1302 General Laws.

1303 (l) The scale and scope of a controller’s cybersecurity program shall be based on:

1304 (1) The size, scope and type of controller obligated to safeguard the personal information  
1305 under such program;

1306 (2) The amount of resources available to the controller;

1307 (3) The amount and nature of personal information processed by the controller; and

1308 (4) The reasonably foreseeable risks to the security and confidentiality of the personal  
1309 information processed by the controller.

1310 (m) The cause of action established by this Section shall apply only to violations as  
1311 defined in this Section. This chapter neither relieves any party from any duties or obligations  
1312 imposed, nor alters any independent rights that individuals have under chapter 93A of the



1313 General Laws, other state or federal laws, the Massachusetts Constitution or the United States  
1314 Constitution.

1315 (n) Nothing in this Section shall limit the authority of the Attorney General to initiate  
1316 actions as otherwise allowed in this Section or pursuant to any other general law.

1317 SECTION 3. Chapter 93M of the General Laws shall take effect 18 months after the  
1318 passage of this act, except that Section 2 and subsections (p) through (w) of Section 25 of said  
1319 chapter shall take effect upon the passage of this act.

1320 SECTION 4. Section 2 of this act shall take effect 18 months after the passage of this act.