HOUSE . . . . No. 60

The Commonwealth of Massachusetts

PRESENTED BY:

Daniel R. Carey

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

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

An Act establishing the Massachusetts information privacy and security act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
Daniel R. Carey	*2nd Hampshire*	*1/20/2023*
Mindy Domb	*3rd Hampshire*	*1/31/2023*

HOUSE . . . . No. 60

By Representative Carey of Easthampton, a petition (accompanied by bill, House, No. 60) of Daniel R. Carey and Mindy Domb relative to the security and the protection of personal information by establishing the Massachusetts information privacy and security act. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

_____

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

_____

An Act 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

9   the context clearly requires otherwise:

10   "Affiliate", an entity that controls, is controlled by, or is under common control or shares

11   common branding with another entity; provided, however, that for the purposes of this definition,

12   "control" or "controlled" shall mean:

13   (1) ownership of more than 50 per cent of the outstanding shares of any class of voting

14   security of the entity;

15   (2) control in any manner over the election of a majority of the entity's directors or of

16   persons exercising similar functions; or

17   (3) the power to otherwise exercise a controlling influence over the management of the

18   entity.

19   "Biometric information", a retina or iris scan, fingerprint, voiceprint, map or scan of hand

20   or face geometry, vein pattern, gait pattern, or other personal information generated from the

21   specific technical processing of an individual's unique biological or physiological patterns or

22   characteristics used to identify a specific individual; provided, however, that "biometric

23   information" shall not include:

24   (1) a digital or physical photograph;

25   (2) an audio or video recording; or

26   (3) data generated from a digital or physical photograph, or an audio or video recording,

27   unless such data is generated to identify a specific individual.

28   "Business associate" shall have the same meaning as in 45 C.F.R. 160.103.

29   "Child", an individual who a controller knows or reasonably should know is under the

30   age of 13.

31   "Collect", buying, renting, gathering, obtaining, receiving, or otherwise accessing any

32   personal information pertaining to an individual by any means, including, but not limited to,

33   obtaining information from an individual, either actively or passively, or by observing an

34   individual's behavior.

35   "Common branding", a shared name, service mark, trademark, or other indicator that an

36   individual would reasonably understand to indicate that two or more entities are commonly

37   owned.

38   "Consent", a clear affirmative act signifying an individual's freely given, specific,

39   informed, and unambiguous agreement to allow the processing of specific categories of personal

40   information relating to the individual for a narrowly defined particular purpose; provided,

41   however, that "consent" may include a written statement, including a statement written by

42   electronic means, or any other unambiguous affirmative action; and provided further, that the

43   following shall not constitute "consent":

44   (1) acceptance of a general or broad terms of use or similar document that contains

45   descriptions of personal information processing along with other, unrelated information;

46   (2) hovering over, muting, pausing, or closing a given piece of content; or

47   (3) agreement obtained through dark patterns or a false, fictitious, fraudulent, or

48   materially misleading statement or representation.

49 "Controller", the entity that, alone or jointly with others, determines the purposes and

50 means of the processing of personal information of an individual.

51 "Covered entity" shall have the same meaning as in 45 C.F.R. 160.103.

52 "Dark pattern", a user interface that is designed, modified, or manipulated with the

53 purpose or substantial effect of obscuring, subverting or impairing a reasonable individual's

54 autonomy, decision-making, or choice.

55 "Data broker", a controller that, in a calendar year, knowingly collects and sells to third

56 parties:

57 (1) the personal information of not less than 25,000 individuals; provided, however, that

58 the controller derives not less than 25 percent of its annual global gross revenues from the sale of

59 personal information;

60 (2) the biometric, genetic, or specific geolocation information of not less than 10,000

61 individuals; or

62 (3) 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: (A) 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; (B)

71   providing publicly available information related to an individual's business or profession; or (C)

72   providing publicly available information via real-time or near-real-time alert services for health

73   or safety purposes.

74   "De-identified information", information that cannot reasonably be used to infer

75   information about, or otherwise be linked to, an identified or identifiable individual or

76   household, or a device linked to such individual or household; provided, however, that the

77   controller that possesses the information:

78   (1) takes reasonable technical and organizational measures to ensure that the information

79   cannot, at any point, be associated with or used to re-identify an identified or identifiable

80   individual or household;

81   (2) publicly commits to process the information solely in a de-identified fashion;

82   (3) does not attempt to re-identify the information; provided, however, that the controller

83   may attempt to re-identify the information solely for the purpose of determining whether its de-

84   identification procedures satisfy the provisions of this definition; and

85   (4) contractually obligates any recipients of the information to comply with the

86   provisions of this definition with respect to the information and requires that such obligations be

87   included contractually in all subsequent instances for which the information may be received.

88   "De-identification", the creation of de-identified information from personal information.

89 "Designated method for submitting a request", a mailing address, email address, internet

90 web page, internet web portal, toll-free telephone number, or other applicable contact

91 information, whereby an individual may submit a request or direction under this chapter.

92 "Entity", a sole proprietorship, or a corporation, association, partnership or other legal

93 entity.

94 "Genetic information", personal information, regardless of format, that:

95 (1) results from the analysis of a biological sample of an individual, or from another

96 source enabling equivalent information to be obtained; and

97 (2) concerns an individual's genetic material, including, but not limited to,

98 deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes,

99 alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs),

100 uninterpreted data that results from analysis of the biological sample or other source, and any

101 information extrapolated, derived, or inferred therefrom.

102 "Health care facility" shall have the same meaning as defined in section 25B of chapter

103 111 of the General Laws.

104 "Health care provider" shall have the same meaning as defined in section 1 of chapter

105 111 of the General Laws.

106 "Health record", an individual's health-related record, as maintained pursuant to section

107 70 of chapter 111 of the General Laws.

108 "HIPAA", the federal Health Insurance Portability and Accountability Act of 1996, 42

109 U.S.C. 1320d et seq., as amended from time to time.

110   "Homepage", the introductory page of an internet website and any internet web page

111   where personal information is collected; provided, however, that in the case of an online service,

112   such as a mobile application, "homepage" shall include:

113   (1) the application's platform page or download page;

114   (2) a link within the application, such as from the application configuration, "About,"

115   "Information," or settings page; and

116   (3) any other location that allows individuals to review the notices required by this

117   chapter, including, but not limited to, before downloading the application.

118   "Identified or identifiable household", a group of individuals who:

119   (1) cohabitate with one another at the same residential address in the commonwealth;

120   (2) use common devices or services; and

121   (3) can be readily identified, directly or indirectly.

122   "Identified or identifiable individual", an individual who can be readily identified,

123   directly or indirectly.

124   "Individual", a natural person who is a resident of the commonwealth; provided,

125   however, that "individual" shall not include a natural person acting as a sole proprietorship.

126   "Infer", deriving information, data, assumptions, correlations, predictions or conclusions

127   from facts, evidence or another source of information or data.

128   "Institution of higher education", any college, junior college, university or other public or

129   private educational institution that has been authorized to grant degrees pursuant to sections 30,

130   30A, and 31A of chapter 69 of the General Laws.

131   "Large data holder", a controller that, in a calendar year:

132   (1) has annual global gross revenues in excess of $1,000,000,000; and

133   (2) determines the purposes and means of processing of the personal information of not

134   less than 200,000 individuals, excluding personal information processed solely for the purpose of

135   completing a payment-only credit, check or cash transaction where no personal information is

136   retained about the individual entering into the transaction.

137   "Minor", an individual who a controller knows or reasonably should know is not less

138   than 13 years of age and not more than 16 years of age.

139   "Nonprofit organization", any organization that is exempt from taxation under 26 U.S.C.

140   501(c), as amended from time to time.

141   "Personal information", information, including, but not limited to, a unique persistent

142   identifier, that identifies, relates to, describes, is reasonably capable of being associated with, or

143   could reasonably be linked, directly or indirectly, with an identified or identifiable individual;

144   provided, however, that "personal information" shall not include publicly available or de-

145   identified information about a natural person; and provided further, that "personal information"

146   shall also include information, including, but not limited to, a unique persistent identifier, that

147   identifies, relates to, describes, is reasonably capable of being associated with, or could

148   reasonably be linked, directly or indirectly, with:

149   (1) an identified or identifiable natural person, only insofar as "personal information" is

150   used in paragraph (1) of the definition of "data broker" in this section; or

151   (2) an identified or identifiable household, only insofar as "personal information" is used

152   in: (i) subsection (b) of section 3; and (ii) any reference in this chapter to the sale or selling of

153   personal information or the processing of personal information for the purposes of targeted

154   cross-contextual or first-party advertising.

155   "Process", any operation or set of operations performed on personal information or on

156   sets of personal information, whether or not by automated means, such as the collection, use,

157   storage, disclosure, sharing, analysis, prediction, deletion or modification of personal

158   information, including the actions of a controller directing a processor to process personal

159   information.

160   "Processor", an entity that processes personal information on behalf of a controller;

161   provided, however, that determining whether an entity is acting as a processor or a controller

162   with respect to a specific processing of personal information is a fact-based determination that

163   depends upon the context in which the information is processed; and provided further, that:

164   (1) a processor that continues to adhere to a controller's instructions with respect to a

165   specific processing of personal information remains a processor;

166   (2) if a processor begins, alone or jointly with others, determining the purposes and

167   means of the processing of personal information, it is a controller with respect to the processing;

168   and

169   (3) an entity that is not limited in its processing of personal information pursuant to a

170   controller's instruction, or that fails to adhere to such instructions, is a controller and not a

171   processor with respect to a specific processing.

172   "Profiling", any form of automated processing of personal information to evaluate,

173   analyze, or predict personal aspects concerning an identified or identifiable individual or

174   household's economic situation, health, personal preferences, interests, reliability, behavior,

175   location or movements.

176   "Protected health information" shall have the same meaning as defined in 45 C.F.R.

177   160.103, established pursuant to HIPAA.

178   "Publicly available information", information about an individual that:

179   (1) is lawfully made available from federal, state, or local government records; or

180   (2) a controller has a reasonable basis to believe is lawfully and intentionally made

181   available to the general public: (i) through widely distributed media; or (ii) by the individual,

182   unless the individual has restricted the information to a specific audience; provided, however,

183   that "publicly available information" shall not include: (A) biometric or genetic information; or

184   (B) personal information that is not publicly available and has been combined with publicly

185   available information.

186   "Research", a systematic investigation, including research development, testing, and

187   evaluation, designed to develop or contribute to generalizable knowledge and that is conducted

188   in accordance with applicable ethics and privacy laws.

189   "Sale" or "selling", disclosing, disseminating, making available, releasing, renting,

190   sharing, transferring, or otherwise communicating orally, in writing, or by electronic or other

191   means, an individual's personal information by the controller to a third party for monetary or

192   other valuable consideration in a bargained-for exchange or otherwise for the purposes of

193   targeted cross-contextual advertising; provided, however, that "sale" or "selling" shall not

194   include the following:

195   (1) the disclosure of personal information to a processor where the processor only

196   processes such personal information on behalf of the controller;

197   (2) the controller's use or sharing of an identifier for an individual who, pursuant to

198   section 8, has opted out of the processing of the individual's personal information; provided,

199   however, that the controller's use or sharing of the identifier is solely for the purpose of alerting

200   entities that the individual has opted out;

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

202   (4) the disclosure or transfer of personal information to a third party as an asset that is

203   part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the

204   third party assumes control of all or part of the controller's assets;

205   (5) the disclosure of personal information to a third party for purposes of providing a

206   product or service specifically requested by the individual; or

207   (6) when the individual uses or expressly directs the controller to disclose personal

208   information to a third party or otherwise interact with a third party; provided, however, that the

209   individual's direction was not obtained through dark patterns; and provided further, that the

210 controller's interaction with the third party is not for the purposes of targeted cross-contextual

211 advertising.

212   "Sensitive information", a form of personal information, including:

213   (1) an individual's specific geolocation information;

214   (2) biometric or genetic information processed for the purpose of uniquely identifying an

215 individual;

216   (3) the personal information of a child or minor;

217   (4) personal information that reveals an individual's: (i) racial or ethnic origin; (ii)

218 religious beliefs; or (iii) citizenship or immigration status;

219   (5) personal information processed concerning an individual's past, present or future

220 mental or physical health condition, disability, diagnosis or treatment;

221   (6) personal information processed concerning an individual's sexual orientation, sex life

222 or reproductive health, including, but not limited to, the use or purchase of contraceptives, birth

223 control, abortifacients or other medication related to reproductive health;

224   (7) personal information that reveals an individual's philosophical beliefs or union

225 membership;

226   (8) personal information that reveals an individual's social security number, driver's

227 license number, military identification number, passport number or state-issued identification

228 card number; or

229   (9) personal information that reveals an individual's financial account number, or credit

230   or debit card number, with or without any required security code, access code, personal

231   identification number or password, that would permit access to an individual's financial account.

232   "Specific geolocation information", information derived from technology including, but

233   not limited to, global positioning system level latitude and longitude coordinates or other

234   mechanisms that directly identify the specific location of an individual within a geographic area

235   that is equal to or less than the area of a circle with a radius of 1,850 feet; provided, however,

236   that "specific geolocation information" shall exclude the content of communications or any

237   information generated by or connected to advanced utility metering infrastructure systems or

238   equipment for use by a utility.

239   "Targeted cross-contextual advertising", the targeting of advertising to an individual

240   based on the individual's personal information obtained from the individual's activity across

241   distinctly-branded internet websites, online applications, services or physical premises; provided,

242   however, that "targeted cross-contextual advertising" shall not include:

243   (1) processing personal information solely for measuring or reporting advertising

244   performance, reach or frequency;

245   (2) contextual advertising that is displayed based on the content in which the

246   advertisement appears and does not vary based on who is viewing the advertisement; or

247   (3) advertising that is based solely on an individual's current intentional interaction with

248   or visit to a controller's distinctly-branded internet website, online application, service or

249   physical premise; provided however, that the individual's personal information is not: (i) used to

250   build a profile about the individual or otherwise alter the individual's experience outside the

251   current intentional interaction with the controller; or (ii) retained after the completion of the

252   interaction; provided further, that an individual's intentional interaction may include, but is not

253   limited to, an individual's current search query or specific request for information and feedback;

254   and provided further, that hovering over, muting, pausing or closing a given piece of content

255   does not constitute an individual's intent to interact with a controller.

256   "Targeted first-party advertising", the targeting of advertising to an individual based on a

257   controller profiling an individual by using the personal information obtained from the

258   individual's activity within a controller's own websites, online applications, services or physical

259   premises; provided, however, that "targeted first-party advertising" shall not include advertising

260   or the processing of personal information pursuant to the exemptions specified in paragraphs (1)

261   through (3) of the definition of targeted cross-contextual advertising.

262   "Third party", a natural person, entity, public authority, agency, or body other than the

263   applicable individual, controller, processor, or affiliate of the controller or the processor.

264   "Trade secret" shall have the same meaning as defined in section 42 of chapter 93 of the

265   General Laws.

266   "Unique persistent identifier", an identifier that is reasonably linkable to an identified or

267   identifiable natural person or household, including, but not limited to, a:

268   (1) device identifier;

269   (2) Internet Protocol address;

270   (3) cookie;

271   (4) beacon;

272   (5) pixel tag;

273   (6) mobile ad identifier or similar technology;

274   (7) customer number;

275   (8) unique pseudonym;

276   (9) user alias;

277   (10) telephone number; or

278   (11) other form of persistent or probabilistic identifier that is linked or reasonably

279   linkable to an identified or identifiable natural person or household.

280   "Upholding security, confidentiality and integrity", protecting against, responding to,

281   preventing, detecting, investigating, reporting or prosecuting identity theft, fraud, harassment,

282   malicious, deceptive or illegal activities, or any other security incidents that compromise the

283   availability, authenticity, confidentiality or integrity of stored or transmitted personal

284   information.

285   "Verifiable request", a request:

286   (1) to exercise any of the rights set forth in sections 10 through 13; and

287   (2) that a controller can use commercially reasonable means to determine is being made

288   by the individual or by a person authorized to exercise rights on behalf of such individual with

289   respect to the personal information at issue, pursuant to section 14.

290   Section 3. Scope and Applicability

291   (a) This chapter shall apply to:

292   (1) a controller or processor that conducts business in the commonwealth; and

293   (2) the processing of personal information by a controller or processor not physically

294 established in the commonwealth, where the processing activities are related to: (i) the offering

295 of goods or services that are targeted to individuals; or (ii) the monitoring of behavior of

296 individuals where such behavior takes place in the commonwealth; and

297   (3) an entity that voluntarily certifies to the attorney general that it is fully in compliance

298 with, and agrees to be bound by, this chapter.

299   (b) Notwithstanding subsection (a) of this section, sections 7 through 17 and section 26

300 shall only apply to a controller that, during the preceding calendar year, satisfied at least 1 of the

301 following additional thresholds or is an entity that is an affiliate of and shares common branding

302 with such a controller, in which case sections 7 through 17 and section 26 shall apply only to the

303 personal information processed by the affiliate on behalf of the controller:

304   (1) the controller had annual global gross revenues in excess of 25,000,000 dollars;

305   (2) the controller was a data broker; or

306   (3) the controller determined the purposes and means of processing of the personal

307 information of not less than 100,000 individuals, excluding personal information processed

308 solely for the purpose of completing a payment-only credit, check or cash transaction where no

309 personal information is retained about the individual entering into the transaction.

310   (c) This chapter shall not apply to:

311   (1) any agency, executive office, department, board, commission, bureau, division or

312   authority of the commonwealth, or any of its branches, or any political subdivision thereof;

313   (2) a national securities association that is registered under 15 U.S.C. 78o-3 of the

314   Securities Exchange Act of 1934, as amended from time to time;

315   (3) a registered futures association that is so designated pursuant to 7 U.S.C. 21, as

316   amended from time to time; and

317   (4) an entity that serves as a congressionally designated nonprofit, national resource

318   center and clearinghouse to assist victims, families, child-serving professionals and the general

319   public on issues concerning missing or exploited children.

320   (d) The following information shall be exempt from this chapter:

321   (1) protected health information that is processed by a covered entity or business

322   associate pursuant to 45 C.F.R. 160, 162, and 164;

323   (2) health records for the purposes of section 70 of chapter 111 of the General Laws, to

324   the extent that the records are maintained pursuant to 45 C.F.R. 160, 162, and 164;

325   (3) information and documents that are created by a covered entity for purposes of

326   complying with HIPAA;

327   (4) information used only for public health activities and purposes as authorized by

328   HIPAA;

329   (5) patient identifying information for purposes of 42 C.F.R. 2, established pursuant to 42

330   U.S.C. 290dd-2, as amended from time to time;

331   (6) information that is: (i) collected for a clinical trial subject to the Federal Policy for the

332   Protection of Human Subjects under 45 C.F.R. 46; (ii) collected pursuant to good clinical

333   practice guidelines issued by the International Council for Harmonisation of Technical

334   Requirements for Pharmaceuticals for Human Use; (iii) collected pursuant to the human subject

335   protection requirements under 21 C.F.R. 50 and 56; or (iv) personal information used or

336   disclosed in research conducted in accordance with one or more of the requirements set forth in

337   this paragraph;

338   (7) information and documents created for purposes of the federal Health Care Quality

339   Improvement Act of 1986, 42 U.S.C. 11101 et seq., as amended from time to time;

340   (8) patient safety work product for purposes of the federal Patient Safety and Quality

341   Improvement Act, 42 U.S.C. 299b-21 et seq., as amended from time to time;

342   (9) information that is: (i) derived from any of the health care-related information listed

343   in this subsection; and (ii) de-identified in accordance with the requirements for de-identification

344   pursuant to 45 C.F.R. 164;

345   (10) information that is treated in the same manner as, or that originates from and is

346   intermingled to be indistinguishable with, information that is exempt under this subsection and

347   maintained by: (i) a covered entity or business associate; (ii) a health care facility or health care

348   provider; or (iii) a program of a qualified service organization as defined by 42 U.S.C. 290dd-2;

349   (11) an activity involving the processing of any personal information bearing on an

350   individual's credit worthiness, credit standing, credit capacity, character, general reputation,

351   personal characteristics or mode of living by: (i) a consumer reporting agency, as defined in 15

352   U.S.C. 1681a(f); (ii) a furnisher of information, as set forth in 15 U.S.C. 1681s-2, that provides

353   information for use in a consumer report, as defined in 15 U.S.C. 1681a(d); and (iii) a user of a

354   consumer report, as set forth in 15 U.S.C. 1681b; provided, however, that this paragraph shall

355   apply only to the extent that: (A) the activity is regulated by the federal Fair Credit Reporting

356   Act, 15 U.S.C. 1681 et seq., as amended from time to time; and (B) the personal information is

357   processed solely as authorized by the federal Fair Credit Reporting Act; and provided further,

358   that the exemption established pursuant to this paragraph shall not apply with respect to section

359   26 of this chapter;

360   (12) personal information processed in compliance with the federal Driver's Privacy

361   Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended from time to time;

362   (13) personal information regulated by the federal Family Educational Rights and Privacy

363   Act, 20 U.S.C. 1232g et seq., as amended from time to time;

364   (14) personal information processed in compliance with the federal Farm Credit Act, 12

365   U.S.C. 2001 et seq., as amended from time to time;

366   (15) personal information processed in compliance with the federal Gramm-Leach-Bliley

367   Act, 15 U.S.C. 6801 et seq., as amended from time to time;

368   (16) personal information processed in compliance with chapter 175I of the General

369   Laws;

370   (17) personal information processed by an air carrier specifically in relation to price,

371   route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq.,

372   as amended from time to time; provided, however, that this exemption shall apply solely to the

373   extent that provisions of this chapter may be preempted by section 41713 of the Airline

374   Deregulation Act; and

375   (18) personal information processed for purposes of chapter 176Q of the General Laws.

376   (e) Section 7 and sections 9 through 13 of this chapter shall not apply to information that

377   is processed:

378   (1) in the course of an individual acting in a professional or commercial context, to the

379   extent that the information is collected and used within that context;

380   (2) in the course of an individual acting as a job applicant to, an employee of, or an agent

381   or independent contractor of a controller, processor, or third party, to the extent that the

382   information is collected and used within the context of the individual's role;

383   (3) as the emergency contact information of an individual acting pursuant to paragraph

384   (2) of this subsection, to the extent that the information is solely used for emergency contact

385   purposes; or

386   (4) in order to administer benefits for another natural person relating to an individual

387   acting pursuant to paragraph (2), to the extent that the information is used solely for the purposes

388   of administering those benefits.

389   Section 4. Conflicting Provisions

390   (a) Wherever possible, law relating to individuals' personal information shall be

391   construed to harmonize with the provisions of this chapter, but in the event of a conflict between

392   the provisions of other laws and this chapter, the provisions that afford the greatest protection for

393   the right of privacy for individuals shall control.

394   (b) Controllers and processors that comply with the verifiable parental consent

395   requirements of the federal Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq., as

396   amended from time to time, shall be in compliance with any obligation to obtain parental consent

397   under this chapter. Nothing in this chapter shall be construed to relieve or change any obligations

398   that a controller, processor, or other entity may have under such Act.

399   Section 5. General Principles for Processing Personal Information

400   (a) Personal information shall be:

401   (1) processed lawfully, fairly and in a transparent manner in relation to the individual and

402   in compliance with this chapter;

403   (2) collected for specified, explicit and legitimate purposes and not further processed in a

404   manner that is incompatible with those purposes;

405   (3) processed in a manner that is adequate, relevant and limited to what is reasonably

406   necessary in relation to the purposes for which it is processed;

407   (4) maintained in a manner such that the information is accurate and, where necessary,

408   kept up to date;

409   (5) maintained in a form which permits identification of individuals for no longer than is

410   necessary for the purposes for which the personal information is processed; and

411   (6) processed in a manner that ensures that the information remains appropriately secure.

412   (b) A controller shall be responsible for complying with subsection (a) by implementing

413   procedures that are reasonable and appropriate, taking into consideration:

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

415   (2) the amount of resources available to the controller;

416   (3) the amount and nature of personal information processed by the controller, including,

417   but not limited to, whether the personal information is sensitive information; and

418   (4) the need for upholding security, integrity and confidentiality with respect to the

419   personal information processed by the controller.

420   (c) A controller that is compliant with the regulations promulgated pursuant to chapter

421   93H of the General Laws with respect to "personal information," as that term is defined in

422   section 1 of said chapter 93H, shall be in compliance with the principle set forth in paragraph (6)

423   of subsection (a) of this section with respect to such personal information.

424   Section 6. Lawful Bases for Processing Personal Information

425   (a) Processing shall be lawful and in compliance with this chapter only if:

426   (1) the individual has given consent to the processing of their personal information for

427   one or more specific purposes;

428   (2) processing is necessary for the performance of a contract to which the individual is

429   party or in order to take steps at the request of the individual prior to entering into a contract;

430   (3) processing is necessary for compliance with a legal obligation to which the controller

431   is subject;

432   (4) processing is necessary in order to protect the vital interests of the individual or of

433   another natural person; provided, however, that the processing cannot be manifestly based on

434   another legal basis and the individual or other natural person is at risk or danger of death or

435   serious physical injury; or

436   (5) processing is necessary for the purposes of the legitimate interests pursued by the

437   controller or by a third party, except where such interests are overridden by the individual's

438   reasonable expectations of privacy or other legal rights; provided, however, that the controller

439   shall conspicuously disclose such processing to the individual in advance and consider the

440   following factors when assessing whether to process personal information pursuant to this

441   paragraph:

442   (i) the context in which the personal information would be collected;

443   (ii) whether the processing is reasonably necessary and proportionate to: (A) provide or

444   maintain a specific product or service requested or reasonably anticipated by the individual to

445   whom the personal information pertains; or (B) perform other specified purposes that are

446   compatible with the reasonable expectations of the individual based on the individual's

447   relationship with the controller;

448   (iii) whether the controller or third party can achieve their legitimate interests in another

449   less intrusive way;

450   (iv) the amount of personal information that would be processed;

451   (v) the nature of the personal information that would be processed, taking into account

452   whether processing the information, such as in the case of processing the business contact

453   information of an individual acting in a commercial or business context, poses minimal risks to

454   the individual;

455   (vi) the possible unlawful disparate impacts and the financial, physical, reputational, or

456   other cognizable harms or consequences for the individual whose personal information would be

457   processed;

458   (vii) whether the processing interferes with an individual's right to privacy pursuant to

459   section 1B of chapter 214 of the General Laws; and

460   (viii) the need for upholding security, integrity and confidentiality with respect to the

461   personal information that would be processed.

462   (b) A controller shall not rely on paragraph (5) of subsection (a) as a lawful basis for

463   processing personal information for the purposes of profiling in furtherance of solely automated

464   decisions that produce legal or similarly significant effects concerning the individual, including,

465   but not limited to, decisions that result in the provision or denial of financial or lending services,

466   housing, insurance, education enrollment or opportunity, criminal justice, employment

467   opportunities, health care services or access to essential goods or services.

468   Section 7. Right to Privacy Notice

469   (a) At or before the point of the collection of an individual's personal information,

470   controllers shall provide the individual with a reasonably accessible, clear and meaningful

471   privacy notice that shall include:

472   (1) a clear and conspicuous description of: (i) whether the controller sells personal

473   information to third parties or processes personal information for the purposes of targeted cross-

474   contextual or first-party advertising; (ii) what categories of sensitive information, if any, the

475   controller processes and for what purposes; (iii) an individual's rights pursuant to sections 8

476   through 13; (iv) how and where individuals may request to exercise these rights; and (v) a link to

477   the attorney general's online mechanism through which the individual may contact the attorney

478   general to submit a complaint pursuant to subsection (p) of section 25;

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

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

481   (4) the categories of personal information, if any, that the controller sells to third parties;

482   (5) the categories of third parties, if any, to whom the controller sells personal

483   information;

484   (6) whether the controller sells personal information to registered data brokers, along

485   with a link to the web page pursuant to paragraph (3) of subsection (p) of section 25;

486   (7) the affiliates to whom the controller discloses personal information;

487   (8) the categories of sources from which personal information is collected;

488   (9) the length of time the controller intends to retain each category of personal

489   information, or, if that is not possible, the criteria used to determine such period; provided,

490   however, that a controller shall retain personal information for a duration consistent with

491   paragraph (5) of subsection (a) of section 5;

492   (10) the effective date of the privacy notice;

493   (11) whether or not any personal information processed by the controller is sold to,

494   processed in, stored in or otherwise accessible to the People's Republic of China, Russia, Iran or

495   North Korea; and

496   (12) a contact method, such as an active email address or other online mechanism, that

497   the individual may use to contact the controller.

498   (b) A controller shall not collect additional categories of personal information or process

499   personal information collected for additional purposes that are incompatible with the disclosed

500   purposes for which the personal information was collected, without providing the individual with

501   notice consistent with subsection (a) of this section.

502   (c) An entity that, acting as a third party, controls the collection of an individual's

503   personal information may satisfy its obligation under this section by providing the required

504   information prominently and conspicuously on the homepage of its internet website; provided,

505   however, that if an entity, acting as a third party, controls the collection of personal information

506   about an individual on its premises, including in a vehicle, then the entity shall, at or before the

507   point of collection, satisfy its obligation under subsection (a) of this section by providing the

508   required information in a clear and conspicuous manner at such location.

509   (d) Nothing in this section shall require a controller to provide the information in a

510   manner that would disclose the controller's trade secrets.

511   (e) The categories of sensitive information required to be disclosed by a controller

512   pursuant to this section shall specifically include each applicable subcategory set forth in

513   paragraphs (1) through (9) in the definition of sensitive information in section 2.

514   (f) A large data holder shall retain and make publicly available on its internet website:

515   (1) copies of previous versions of its privacy notices for at least 10 years; and

516   (2) a log describing the date and nature of each change to its privacy notice that is likely

517   to affect a reasonable individual's decision or conduct regarding a large data holder's product or

518   service.

519   (g) Subsection (f) shall only apply to privacy notices created or generated after the

520   effective date of this section and shall not be retroactive.

521   Section 8. Opting Out of the Sale of Personal Information and Targeted Advertising

522   (a) An individual shall have the right to opt out of the processing of the individual's

523   personal information for the purposes of:

524   (1) the sale of the personal information;

525   (2) targeted cross-contextual advertising; or

526   (3) targeted first-party advertising.

527   (b) A controller shall comply with an opt-out request pursuant to this section as soon as

528   reasonably possible; provided, however, that a controller shall comply with an opt-out request

529   with respect to paragraph (1) of subsection (a) in a time frame that is reasonably proportionate to

530   the amount of time it takes the controller to sell such personal information to third parties; and

531   provided further, that in any event, a controller shall comply with an opt-out request pursuant to

532   this section not later than 15 days after receipt of the request.

533   (c) A controller that has received an opt-out request pursuant to this section shall be

534   prohibited from processing the individual's personal information for the purposes of the sale of

535   the personal information or for targeted cross-contextual or first-party advertising, unless the

536   individual subsequently provides consent for such processing. After complying with an

537   individual's opt-out request, a controller shall wait for not less than 12 months before requesting

538   the individual's consent to process the individual's personal information for the purposes of the

539   sale of the personal information or for targeted cross-contextual or first-party advertising.

540   (d) A data broker that has been sold an individual's personal information shall not further

541   process an individual's personal information for the purposes of the sale of the personal

542   information or for targeted cross-contextual advertising, unless the individual has received

543   explicit notice and is provided an opportunity to exercise the opt-out right pursuant to this

544   section.

545   (e) If a controller communicates to any entity authorized by the controller to collect

546   personal information that an individual has requested to exercise the opt-out right pursuant to this

547   section, that entity shall thereafter only use that individual's personal information for purposes

548   specified by the controller, or as otherwise permitted by this chapter, and shall be prohibited

549   from:

550   (1) processing the individual's personal information for the purposes of the sale of the

551   personal information or for targeted cross-contextual or first-party advertising; and

552   (2) processing that individual's personal information: (i) outside of the direct relationship

553   between the entity and the controller; or (ii) for any purpose other than for the specific purpose

554   of providing or performing the services offered to the controller.

555   (f) A controller that pursuant to subsection (e) communicates an individual's opt-out

556   request to an entity shall not be liable under this chapter if the entity receiving the opt-out request

557   violates the restrictions set forth in this chapter; provided, however, that at the time of

558   communicating the opt-out request, the controller does not know or should not reasonably know

559   that the entity intends to commit such a violation.

560   (g) An individual may designate an authorized agent to act on the individual's behalf to

561   opt out of the processing of such individual's personal information for one or more of the

562   purposes specified in subsection (a). The individual may designate such authorized agent by way

563   of, among other things, a technology, including, but not limited to, an internet link or a browser

564   setting, browser extension or global device setting, indicating the individual's intent to opt out of

565   such processing. A controller shall comply with an opt-out request received from an authorized

566   agent if the controller is able to verify, with commercially reasonable effort, the authorized

567   agent's authority to act on the individual's behalf. An authorized agent shall:

568   (1) not use an individual's personal information for any purposes other than to fulfill the

569   individual's requests, for verification or for fraud prevention; and

570   (2) implement and maintain reasonable security procedures and practices to protect the

571   individual's personal information.

572   (h) A controller shall allow an individual to opt out of the processing of the individual's

573   personal information for one or more of the purposes specified in subsection (a) through an opt-

574   out preference signal sent with the individual's consent to the controller by a platform,

575   technology or mechanism indicating the individual's intent to opt out of such processing;

576   provided, however, that such platform, technology or mechanism shall meet the requirements

577   and technical specifications established by the attorney general pursuant to subsection (u) of

578   section 25; and provided further, that a controller shall notify individuals about any such

579   platform, technology or mechanism in any privacy notice provided pursuant to section 7.

580   (i) If an individual decides to opt out of the processing of the individual's personal

581   information for one or more of the purposes specified in subsection (a) through an opt-out

582   preference signal sent in accordance with this chapter and the individual's decision conflicts with

583   the individual's existing controller-specific privacy setting or voluntary participation in the

584   controller's bona fide loyalty, rewards, premium features, discounts or club card program, the

585   controller shall comply with the individual's opt-out preference signal but may notify the

586   individual of the conflict and provide the individual with the choice to opt back into such

587   controller-specific privacy setting or participation in such a program; provided, however, that the

588   controller shall not use dark patterns to coerce the individual to opt back in to such controller-

589   specific privacy setting or participation in such program.

590   (j) If a controller responds to an individual's opt-out request pursuant to this section by

591   informing the individual of a charge for the use of any product or service, the controller shall

592   present the terms of any financial incentive offered in accordance with section 16 for the

593   collection, processing, sale or retention of the individual's personal information.

594   (k) A request to exercise the right to opt out pursuant to this section shall not need to be a

595   verifiable request. If a controller, however, has a good-faith, reasonable and documented belief

596   that the request is fraudulent, the controller may deny the request. The controller shall inform the

597   requestor that it will not comply with the request and shall provide an explanation why it

598   believes the request is fraudulent.

599   (l) For each calendar year in which a controller is a large data holder, the controller shall

600   prepare a report that details the number of requests that is has received to opt out pursuant to

601   paragraphs (1), (2) and (3) of subsection (a); provided, however, that the controller shall specify

602   the number of such requests that the controller has denied; and provided further, that the

603   controller shall make its report publicly available on its internet website and submit the report to

604   the attorney general not later than January 31 following each year in which a controller meets the

605   definition of a large data holder under this chapter.

606   Section 9. Protections for Sensitive Information

607   (a) A controller shall not process an individual's sensitive information for the purposes of

608   the sale of such information or for targeted cross-contextual or first-party advertising, unless the

609   controller has obtained the consent of the individual, or, in the case of a child, the child's parent

610   or guardian.

611   (b) A controller shall not otherwise process an individual's sensitive information without

612   first obtaining the consent of the individual, or, in the case of a child, the child's parent or

613   guardian, except to the limited extent necessary to:

614   (1) perform the services or provide the goods reasonably expected by an average

615   individual who requests those services or goods;

616   (2) maintain or service accounts, provide customer service, process or fulfill orders and

617   transactions, verify customer information, process payments, provide financing, provide analytic

618   services, provide storage or provide other similar services;

619   (3) verify, maintain, improve or upgrade the quality or safety of the service or device that

620   is owned, manufactured, manufactured for or controlled by the controller; or

621   (4) perform short-term, transient use, including, but not limited to, advertising that is

622   based solely on an individual's personal information derived from the individual's current

623   intentional interaction with the controller; provided, however, that the sensitive information shall

624   not be an individual's precise geolocation information; and provided further, that the individual's

625   sensitive information shall not be: (i) disclosed to another third party; or (ii) used to build a

626   profile about the individual or otherwise alter the individual's experience outside the current

627   interaction with the controller; or

628   (5) otherwise process the information pursuant to an exemption stipulated in section 24.

629   (c) If a controller does not receive consent for the processing of an individual's sensitive

630   information, the controller shall wait for not less than 12 months before making a subsequent

631   request for the individual or, in the case of a child, the child's parent or guardian, to consent to

632   such processing.

633   Section 10. Right to Access and Transport Personal Information

634   (a) For the purposes of this section, "specific pieces of information" shall not include any

635   data generated to uphold security, confidentiality and integrity.

636   (b) An individual shall have the right to request that a controller that processes the

637   individual's personal information disclose to the individual the specific pieces of personal

638   information that the controller has processed about the individual, including inferences linked or

639   reasonably linkable to the individual.

640   (c) In response to a verifiable request pursuant to subsection (b), a controller shall

641   provide to the individual the specific pieces of personal information that the controller has

642   processed about the individual in a portable format that is easily understandable to the average

643   individual and, to the extent technically feasible, in a readily usable format that allows the

644   individual to transmit the information to another controller without hindrance.

645   (d) The disclosure of the required information pursuant to this section shall cover the 12-

646   month period preceding the controller's receipt of the verifiable request; provided, however, that

647   an individual may request that the controller disclose the required information beyond the 12-

648   month period, and the controller shall be required to provide such information unless doing so

649   proves impossible or would constitute an undue burden for the controller; and provided further,

650   that an individual's ability to request information beyond the 12-month period shall be disclosed

651   in a controller's privacy notice pursuant to clause (iii) of paragraph (1) of subsection (a) of

652   section 7.

653   (e) Nothing in this section shall require a controller to provide the information requested

654   in a manner that would disclose the controller's trade secrets.

655   Section 11. Right to Delete Personal Information

656   (a) An individual shall have the right to request that a controller delete any personal

657   information processed about the individual.

658   (b) A controller that receives a verifiable request to delete the individual's personal

659   information shall:

660   (1) delete the individual's personal information from its records;

661   (2) notify all processors to whom the controller has disclosed the individual's personal

662   information to delete the individual's personal information from their records; and

663   (3) notify all third parties to whom the controller has sold the individual's personal

664   information to delete the personal information from their records, unless doing so proves

665   impossible or would constitute an undue burden for the controller.

666   (c) A controller may maintain a confidential record of deletion requests solely for:

667   (1) preventing the sale of the personal information of the individual who has submitted a

668   deletion request;

669   (2) ensuring that such individual's personal information is deleted from the controller's

670   records; or

671   (3) other purposes to the extent permissible pursuant to section 24 and subsection (i) of

672   section 15.

673   (d) A controller, or a processor acting pursuant to its contract with the controller, shall

674   not be required to comply with an individual's request to delete the individual's personal

675   information if it is reasonably necessary for the controller or processor to maintain the

676   individual's personal information in order to:

677   (1) complete the transaction for which the personal information was collected, provide a

678   good or service requested by the individual or reasonably anticipated by the individual within the

679   context of the controller's ongoing relationship with the individual, or otherwise perform a

680   contract between the controller and the individual;

681   (2) enable solely internal uses that are: (i) reasonably aligned with the expectations of the

682   individual based on the individual's relationship with the controller; and (ii) compatible with the

683   context in which the individual provided the personal information;

684   (3) maintain personal information that relates to a public figure and for which the

685   individual making the deletion request has no reasonable expectation of privacy; or

686   (4) comply with a legal obligation or otherwise process personal information pursuant to

687   an exemption stipulated in section 24.

688   (e) The controller or processor shall retain personal information pursuant to subsection

689   (d) solely for the applicable purposes under that subsection.

690   Section 12. Right to Correct Personal Information

691   (a) An individual shall have the right to request that a controller correct inaccurate

692   personal information processed about the individual, taking into account the nature of the

693   personal information and the purposes of the processing of such information.

694   (b) A controller that receives a verifiable request to correct inaccurate personal

695   information shall correct the inaccurate personal information as directed by the individual.

696   Section 13. Right to Revoke Consent

697   (a) If a controller chooses to process an individual's personal information on the basis of

698   the individual's consent pursuant to paragraph (1) of subsection (a) of section 6, the option for an

699   individual to refuse consent shall be clear, at least as prominent as the option to accept, and easy

700   to use by a reasonable individual.

701   (b) In addition to an individual's opt-out right pursuant to section 8, an individual shall

702   have the right to revoke consent that the individual previously gave to a controller to process the

703   individual's personal information for any other purposes. The controller shall:

704   (1) provide a mechanism for individuals to revoke consent that is clear, conspicuous and

705   easy to use by a reasonable individual; and

706   (2) in response to an individual's verifiable request to revoke the individual's consent,

707   cease to process the individual's personal information as soon as reasonably possible.

708   Section 14. Exercising Privacy Rights

709   (a) An individual may exercise the rights set forth in sections 8 through 13 by submitting

710   a request, at any time, to a controller specifying which rights the individual wishes to exercise.

711   (b) With respect to the processing of personal information of a child, the child's parent or

712   legal guardian may exercise the rights set forth in sections 8 through 13 on the child's behalf.

713   (c) With respect to the processing of personal information concerning an individual

714   subject to guardianship, conservatorship or other protective arrangement under article V or

715   article 5A of chapter 190B of the General Laws, the individual's guardian or conservator may

716   exercise the rights set forth in sections 8 through 13 on the individual's behalf.

717   Section 15. Responding to Requests to Exercise Privacy Rights

718   (a) Except as otherwise provided in this chapter, a controller shall comply with an

719   individual's request to exercise the rights set forth in sections 10 through 13.

720   (b) A controller shall inform the individual of any action taken on a request to exercise

721   any of the rights set forth in sections 10 through 13 without undue delay and in any event within

722   45 days of receipt of the request; provided, however, that the period may be extended once by 45

723   additional days where reasonably necessary, taking into account the complexity and number of

724   the requests; and provided further, that the controller shall notify the individual of any such

725   extension within 45 days of receipt of the request, together with the reasons for the delay.

726   (c) A controller shall not be obligated to comply with a request to exercise the rights set

727   forth in sections 10 through 13 if the request is not a verifiable request. In such a case, the

728   controller shall notify the individual that it is unable to act on the request until it receives

729   additional information reasonably necessary to verify that the request is being made by the

730   individual or by another person who is entitled to exercise such rights on behalf of the individual

731   pursuant to section 14.

732   (d) A verifiable request to exercise the rights set forth in sections 10 through 13 shall not

733   extend to personal information about the individual that belongs to, or the controller maintains

734   on behalf of, another natural person. A controller may rely on representations made in a

735   verifiable request as to rights with respect to personal information and shall not be required to

736   seek out other persons that may have or claim to have rights to personal information or to take

737   any action under this chapter in the event of a dispute between or among persons claiming rights

738   to personal information in the controller's possession.

739   (e) When a controller, pursuant to section 23, is incapable of complying with an

740   individual's verifiable request, the controller shall, if possible, notify the individual that it is

741   unable to identify the individual and cannot act on the request. The individual, or a person

742   entitled to exercise the rights of this chapter on behalf of the individual pursuant to section 14,

743   may provide additional information to the controller enabling the individual's identification for

744   the purposes of exercising the rights set forth in sections 10 through 13.

745   (f) If a controller declines to take action regarding an individual's request, the controller

746   shall notify the individual of the justification for declining to take action and provide the

747   individual with instructions on how to submit a complaint pursuant to subsection (i) of this

748   section. Such notification shall occur without undue delay, but not later than 45 days after the

749   initial receipt of the request or not later than 45 days after notifying the individual of the

750   applicability of an extension pursuant to subsection (b).

751   (g) A controller shall not be obligated to provide the information required by section 10

752   to the same individual more than twice in a 12-month period. Information provided in response

753   to a request shall be provided by the controller to the individual free of charge.

754   (h) If requests from an individual, or from a person entitled to exercise the rights of this

755   chapter on behalf of such individual pursuant to section 14, are manifestly unfounded, excessive

756   or repetitive, the controller may: (1) charge a reasonable fee to cover the administrative costs of

757   complying with the request; or (2) refuse to act on the request. The controller shall bear the

758   burden of demonstrating the manifestly unfounded or excessive nature of the request.

759   (i) When informing an individual of any action taken or not taken in response to a

760   request, the controller shall provide the individual with a link to the attorney general's online

761   mechanism through which the individual may contact the attorney general to submit a complaint.

762   The controller shall maintain records of all rejected requests for not less than 24 months and shall

763   compile and provide a copy of such records to the attorney general upon the attorney general's

764   request.

765   Section 16. Non-Discrimination Against Individuals' Good Faith Exercise of Privacy

766   Rights

767   (a) A controller shall not discriminate against an individual for exercising in good faith

768   any of the rights set forth in this chapter, including, but not limited to, by:

769   (1) denying goods or services to the individual;

770   (2) charging different prices or rates for goods or services, including through the use of

771   discounts or other benefits or imposing penalties;

772   (3) providing a different level of quality of goods or services to the individual;

773   (4) suggesting that the individual will receive a different price or rate for goods or

774   services or a different level of quality or goods or services; or

775   (5) retaliating against a job applicant to, an employee of, or an agent or independent

776   contractor of the controller for exercising their rights under this chapter.

777   (b) This section shall not prohibit a controller from offering a different price, rate, level,

778   quality or selection of goods or services to an individual, including offering goods or services for

779   no fee, if:

780   (1) the offering is in connection with an individual's voluntary participation in a bona

781   fide loyalty, rewards, premium features, discounts or club card program; and

782   (2) the difference is reasonably related to the value provided to the controller by the

783   individual's personal information.

784   (c) Nothing in this section shall be construed to:

785   (1) require a controller to provide a product or service that requires an individual's

786   personal information that the controller does not process; or

787   (2) prohibit a controller from offering a financial incentive, including payments to

788   individuals as compensation, for the processing of personal information; provided, however, that

789   such payments shall be reasonably related to the value provided to the controller by the

790   individual's personal information.

791   Section 17. Disclosure of Methods for Exercising Privacy Rights

792   (a) A controller shall make available and describe in a privacy notice pursuant to section

793   7 not less than 2 designated methods for submitting a request to exercise the rights set forth in

794   sections 8 through 13. The designated methods shall be reasonably accessible to individuals and

795   take into account the ways in which individuals interact with the controller, the need for secure

796   and reliable communication of the request, and the ability of the controller to determine whether

797   the request is a verifiable request. If a controller maintains an internet website, the controller

798   shall make its website available as one such designated method for submitting a request. A

799   controller shall not require an individual to create a new account but may require an individual to

800   use an existing account in order to exercise a right under this chapter.

801   (b) A controller that processes personal information for the purposes of selling such

802   information or for targeted cross-contextual advertising shall provide a clear and conspicuous

803   link on the controller's internet homepages to an internet web page that enables an individual, or

804   an individual's authorized agent, to exercise their right to opt out of such processing.

805   (c) A controller that processes personal information for the purposes of targeted first-

806   party advertising shall provide a clear and conspicuous link on the controller's internet

807   homepages to an internet web page that enables an individual, or an individual's authorized

808   agent, to exercise their right to opt out of such processing.

809   (d) In lieu of complying with both subsections (b) and (c), a controller that is subject to

810   both subsections may utilize a single clearly labeled link on the controller's internet homepages,

811   if that link easily allows an individual, or an individual's authorized agent, to exercise their right

812   to opt out of the processing of the individual's personal information for the purposes of the sale

813   of such information and for targeted cross-contextual and first-party advertising.

814   (e) A controller shall:

815   (1) ensure that all persons responsible for handling individuals' inquiries about the

816   controller's privacy practices or compliance with this chapter are informed of: (i) all

817   requirements set forth under this chapter; and (ii) how to direct individuals to exercise their

818   rights set forth in sections 8 through 13 of this chapter;

819   (2) include a separate link to the applicable web pages required under subsections (b), (c),

820   or (d) of this section in any privacy notice that the controller is required to provide to individuals

821   pursuant to section 7;

822   (3) process any personal information collected from the individual in connection with the

823   submission of the individual's request to exercise any of the rights set forth in sections 8 through

824   13 solely for the purposes of complying with the request;

825   (4) process any personal information collected in connection with the controller's

826   verification of the individual's request solely for the purposes of verification and not further

827   disclose the personal information, retain it longer than necessary for purposes of verification or

828   use it for unrelated purposes;

829   (5) not require an individual to provide additional information beyond what is necessary

830   to direct the controller, pursuant to section 8, to not process the individual's personal information

831   for the purposes of the sale of such information or for targeted cross-contextual or first-party

832   advertising; and

833   (6) not condition, effectively condition, attempt to condition or attempt to effectively

834   condition the exercise of the rights set forth in sections 8 through 13 through the use of dark

835   patterns or any false fictitious, fraudulent or materially misleading statement or representation.

836   Section 18. No Waiver

837   Any provision of a contract or agreement that purports to waive or limit in any way

838   individual rights under this chapter shall be deemed contrary to public policy and shall be void

839   and unenforceable.

840   Section 19. Relationship Among Controllers, Processors and Third Parties

841   (a) A processor shall not be required to comply with a request to exercise the rights set

842   forth in sections 8 through 13 that the processor receives directly from an individual, or from a

843   person entitled to exercise such rights on behalf of the individual, to the extent that the processor

844   has processed the individual's personal information on behalf of the controller.

845   (b) A processor shall adhere to the instructions of the controller and assist the controller

846   in meeting its obligations under this chapter. Taking into account the nature of the processing

847   and with respect to the personal information available to the processor as a result of its

848   relationship with the controller, a processor shall:

849   (1) take appropriate technical and organizational measures, insofar as is possible, to fulfill

850   the controller's obligation to respond to individuals' requests to exercise their rights pursuant to

851   sections 8 through 13;

852   (2) provide information to the controller necessary to enable the controller to conduct and

853   document any risk assessment required by section 21; and

854   (3) assist the controller in meeting the controller's obligations in relation to the security

855   of processing the personal information and in relation to the notification of a breach of security

856   of the system of the processor pursuant to chapter 93H of the General Laws; provided, however,

857   that the controller and the processor shall: (i) implement appropriate technical and organizational

858   measures to ensure a level of security appropriate to the risk; and (ii) establish a clear allocation

859   of the responsibilities between them to implement such measures.

860   (c) When working with the controller to respond to a verifiable request to delete an

861   individual's personal information, the processor shall notify any processors or third parties who

862   may have accessed the personal information from or through the processor to delete the personal

863   information, unless the information was accessed at the direction of the controller or unless

864   doing so proves impossible or would constitute an undue burden.

865   (d) Notwithstanding the instructions of the controller, a processor shall ensure that each

866   person processing personal information is subject to a duty of confidentiality with respect to the

867   information.

868   (e) If a processor engages another entity to assist the processor in processing personal

869   information on behalf of the controller, the processor shall provide the controller with an

870   opportunity to object and the engagement shall be pursuant to a written contract, in accordance

871   with the provisions of subsection (f), that requires the entity to meet the obligations of the

872   processor with respect to the personal information.

873   (f) A contract between a controller and a processor shall govern the processor's

874   procedures with respect to processing individuals' personal information that the processor

875   receives from or on behalf of the controller. The contract shall be binding on both parties and

876   clearly set forth the processing instructions to which the processor is bound, including:

877   (1) the nature and purpose of the processing;

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

879   (3) the duration of the processing;

880   (4) the rights and obligations of both parties;

881   (5) the requirements imposed by subsections (d) and (e); and

882   (6) the following requirements:

883   (i) at the controller's direction, the processor shall delete or return all personal

884   information to the controller as requested at the end of the provision of services, unless retention

885   of the personal information is required by law;

886   (ii) upon the reasonable request of the controller, the processor shall make available to

887   the controller all information in its possession necessary to demonstrate compliance with the

888   obligations under this chapter;

889   (iii) the processor shall: (A) allow for, and cooperate with, reasonable audits and

890   inspections by the controller or the controller's designated auditor; or (B) arrange for, with the

891   controller's consent, a qualified and independent auditor to conduct, at least annually and at the

892   processor's expense, an audit of the processor's policies and technical and organizational

893   measures in support of the obligations under this chapter using an appropriate and accepted

894   control standard or framework and audit procedure for such audits; provided, however, that the

895   processor shall disclose a report of the audit to the controller upon request; and

896   (iv) the processor shall be prohibited from: (A) selling the personal information; (B)

897   processing personal information other than for the purposes specified in the contract or as

898   otherwise permitted by this chapter; (C) processing personal information outside of the direct

899   relationship between the processor and the controller; or (D) combining, for the purpose of

900   targeted advertising, the personal information with the personal information that the processor

901   receives from, or on behalf of, another entity or that it collects from its own interaction with the

902   individual.

903   (g) In no event may any contract relieve a controller or a processor from the liabilities

904   imposed on it by this chapter.

905   (h) A controller shall exercise reasonable due diligence in:

906   (1) selecting a processor; and

907   (2) deciding whether to sell personal information to a third party.

908   Section 20. Data Broker Registration

909   (a) Not later than January 31 following each year in which a controller meets the

910   definition of a data broker under this chapter, the controller shall register with the attorney

911   general pursuant to the requirements of this section.

912   (b) When registering with the attorney general, a data broker shall pay a registration fee

913 of 200 dollars and provide the following information:

914   (1) the data broker's name and primary physical, email and internet website addresses;

915   (2) any privacy notice that the data broker discloses to individuals pursuant to section 7;

916   (3) how individuals may request to exercise their rights under sections 8 through 13;

917   (4) whether the data broker implements a purchaser credentialing process;

918   (5) whether the data broker processes the personal information of minors or children;

919   (6) whether it qualifies as a data broker pursuant to paragraph (1), (2) or (3) of the

920 definition of data broker in section 2;

921   (7) whether the data broker is a large data holder; and

922   (8) any additional information the data broker may wish to provide.

923   Section 21. Risk Assessments

924   (a) A controller shall establish, implement and maintain reasonable policies, practices and

925 procedures to identify, assess and mitigate reasonably foreseeable privacy risks and cognizable

926 harms related to their products and services, including the design, development and

927 implementation of such products and services.

928   (b) A controller shall, prior to the processing, carry out and document a risk assessment

929 of the impact of each of the following processing operations:

930   (1) processing personal information for the purposes of: (i) the sale of the personal

931   information; (ii) targeted cross-contextual advertising; or (iii) targeted first-party advertising;

932   (2) processing personal information for the purposes of profiling or otherwise

933   systematically and extensively evaluating personal aspects relating to individuals; provided,

934   however, that such processing presents a reasonably foreseeable risk of resulting in:

935   (i) discrimination on the basis of race, color, religion, national origin, sex or disability or

936   other unfair or deceptive treatment of, or unlawful disparate impact on, individuals;

937   (ii) financial, physical or reputational harm to individuals;

938   (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or

939   concerns, of individuals, where such intrusion would be offensive to a reasonable person; or

940   (iv) other substantial cognizable harms to individuals;

941   (3) processing sensitive information; and

942   (4) any other processing that is likely to result in a high risk of harm to individuals, taking

943   into account the nature, scope, context, and purposes of the processing and whether the

944   processing involves new technologies.

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

946   (1) a systematic description of the envisioned processing operations and the purposes of

947   the processing, including, where applicable, the legitimate interest pursued by the controller or

948   third party;

949   (2) a description and brief justification of the lawful basis, pursuant to section 6, that the

950   controller is relying on to process the individual's personal information;

951   (3) an assessment of the necessity of the processing operations in relation to the purposes,

952   taking into account whether the controller or third party can achieve their legitimate interests in

953   another less intrusive way;

954   (4) an assessment of the proportionality of the processing operations in relation to the

955   purposes, taking into account the amount and nature of the personal information to be processed;

956   (5) a description of: (i) the context of the processing; (ii) the relationship between the

957   controller and the individual whose personal information would be processed; and (iii) whether

958   the controller is processing an individual's personal information in ways in which the individual

959   would reasonably expect;

960   (6) an assessment of the risks of the processing operations to individuals; provided,

961   however, that such assessment shall include, but not be limited to, whether the processing: (i)

962   poses reasonably foreseeable risks to children or minors; (ii) presents a reasonably foreseeable

963   risk of disparate impact on the basis of individuals' race, color, religion, national origin, sex or

964   disability; or (iii) would result in the provision or denial of financial or lending services, housing,

965   insurance, education enrollment or opportunity, criminal justice, employment opportunities,

966   health care services or access to essential goods or services; and

967   (7) the measures envisioned to mitigate the risks, including, but not limited to, safeguards

968   such as de-identification and security measures to ensure the protection of personal information

969   in compliance with this chapter, taking into account the individuals' reasonable expectations of

970   privacy or other legal rights.

971   (d) In any risk assessment required pursuant to this section, a large data holder shall also:

972   (1) specify whether the processing is based in whole or in part on an algorithmic

973   computational process that:

974   (i) uses machine learning, natural language processing, artificial intelligence techniques

975   or other techniques of similar or greater complexity;

976   (ii) makes a decision or facilitates human decision-making with respect to personal

977   information, including decisions that determine the provision of products or services or that rank,

978   order, promote, recommend, amplify or similarly determine the delivery or display of

979   information to an individual; and

980   (iii) poses a reasonably foreseeable risk of substantial cognizable harm to individuals; and

981   (2) include a description of:

982   (i) the design process and methodologies of any such algorithmic computational process

983   pursuant to paragraph (1);

984   (ii) the categories of data that would be processed as input or used to train the model that

985   any such algorithmic computational process relies on; and

986   (iii) the outputs that would be produced by any such algorithmic computational process.

987   (e) Subsections (a) through (d) shall not apply to processing:

988   (1) that a controller performs pursuant to paragraph (3) of section 6; and

989   (2) for which the controller has already carried out a risk assessment for the purpose of

990   compliance with another applicable law that regulates the specific processing operation or set of

991   operations in question; provided, however, that such assessment has reasonably comparable

992   scope and effect to the assessment that would otherwise be conducted pursuant to this section.

993   (f) For the purpose of complying with this section, a controller may leverage its existing

994   work product of risk assessments that the controller has conducted or is conducting for the

995   purpose of complying with another applicable law.

996   (g) A single risk assessment may address a set of similar processing operations that

997   present similar high risks.

998   (h) The controller shall carry out a review of the risk assessment if there is a change of

999   the risk represented by the processing operations.

1000   (i) A controller shall implement procedures to comply with this section that are

1001   reasonable and appropriate taking into consideration:

1002   (1) the size, scope, and type of the controller;

1003   (2) the amount of resources available to the controller;

1004   (3) the amount and nature of personal information processed by the controller, including,

1005   but not limited to, whether the personal information is sensitive information; and

1006   (4) the need for upholding security, integrity and confidentiality with respect to the

1007   personal information processed by the controller.

1008   (j) The attorney general may require, pursuant to a civil investigative demand, that a

1009   controller disclose any risk assessment that is relevant to an investigation conducted by the

1010   attorney general. The controller shall accordingly make the risk assessment available to the

1011   attorney general, who may evaluate the risk assessment for compliance with the responsibilities

1012   set forth in this chapter. Risk assessments shall be confidential and exempt from public

1013   inspection and copying under chapter 66 of the General Laws. The disclosure of a risk

1014   assessment pursuant to a civil investigative demand from the attorney general shall not constitute

1015   a waiver of attorney-client privilege or work product protection with respect to the assessment

1016   and any information contained in the assessment.

1017   (k) Risk assessments shall apply to processing activities created or generated after the

1018   effective date of this section and shall not be retroactive.

1019   Section 22. Processing That Unlawfully Discriminates

1020   (a) A controller shall not process personal information in a manner that discriminates in,

1021   or otherwise makes unavailable, the equal enjoyment of goods or services on the basis of race,

1022   color, religion, national origin, sex or disability.

1023   (b) A controller that processes personal information in a manner that violates chapter

1024   151B of the General Laws or any other state or federal law prohibiting unlawful discrimination

1025   against individuals shall also be in violation of this chapter.

1026   (c) Nothing in this section shall be construed to limit controllers from processing personal

1027   information for the purpose of:

1028   (1) legitimate testing to prevent unlawful discrimination or otherwise determine the

1029   extent or effectiveness of the controller's compliance with this section; or

1030   (2) diversifying an applicant, participant or customer pool.

1031   (d) This section shall not apply to any private club or group not open to the public,

1032   pursuant to section 201(e) of the Civil Rights Act of 1964, 42 U.S.C. 2000a(e), as amended from

1033   time to time.

1034   Section 23. De-Identified Information

1035   This chapter shall not be construed to require a controller or processor to do any of the

1036   following solely for the purpose of complying with this chapter:

1037   (1) maintain information in an identifiable, linkable or associable form, or collect, obtain,

1038   retain or access any information or technology, in order to be capable of linking or associating a

1039   verifiable request with personal information; or

1040   (2) reidentify or otherwise link de-identified information; provided, however, that the

1041   controller, pursuant to subsection (e) of section 15, shall provide applicable notice to the

1042   individual that it is unable to identify the individual.

1043   Section 24. Limitations

1044   (a) The obligations imposed on controllers or processors under this chapter shall not

1045   restrict a controller's or a processor's ability to:

1046   (1) comply with federal, state or local laws, rules or regulations;

1047   (2) comply with a civil, criminal or regulatory inquiry, subpoena or summons by federal,

1048   state, local or other governmental authorities;

1049   (3) cooperate with law enforcement agencies concerning conduct or activity that the

1050   controller or processor reasonably and in good faith believes may violate federal, state or local

1051   laws, rules or regulations;

1052   (4) investigate, establish, exercise, prepare for or defend legal claims.

1053   (5) take immediate steps to protect the security or protection of an individual or another

1054   natural person, if that individual or other natural person is at risk or danger of death or serious

1055   physical injury;

1056   (6) process the personal information of a child or minor solely in order to submit

1057   information relating to child victimization to law enforcement or to the nonprofit, national

1058   resource center and clearinghouse congressionally designated to provide assistance to victims,

1059   families, child-serving professionals and the general public on missing and exploited children

1060   issues; or

1061   (7) assist another controller, processor or third party with any of the obligations under

1062   this subsection.

1063   (b) The obligations imposed on controllers or processors under sections 8 through 13

1064   shall not restrict a controller or processor's ability to process personal information for the

1065   following purposes, provided that the use of the individual's personal information is reasonably

1066   necessary and proportionate for such purposes:

1067   (1) helping to uphold security, confidentiality and integrity;

1068   (2) debugging to identify and repair errors that impair existing intended functionality;

1069   (3) fulfilling the terms of a written warranty or product recall conducted in accordance

1070   with federal law;

1071   (4) engaging in public or peer-reviewed scientific, historical or statistical research in the

1072   public interest that conforms or adheres to all other applicable ethics and privacy laws; provided,

1073   however, that such research is approved, monitored and governed by an institutional review

1074   board, human subjects research ethics review board or a similar independent oversight entity that

1075   determines whether:

1076   (i) the research is likely to provide substantial benefits that do not exclusively accrue to

1077   the controller;

1078   (ii) the expected benefits of the research outweigh the privacy risks; and

1079   (iii) the controller has implemented reasonable safeguards to mitigate privacy risks

1080   associated with research, including any risks associated with reidentification.

1081   (c) Obligations imposed on controllers or processors under this chapter shall not:

1082   (1) apply to the processing of personal information by a natural person in the course of a

1083   purely personal or household activity;

1084   (2) apply where compliance by the controller or processor would violate an evidentiary

1085   privilege under the laws of the commonwealth or be construed to prevent a controller or

1086   processor from providing personal information concerning an individual to a person covered by

1087   an evidentiary privilege under the laws of the commonwealth as part of a privileged

1088   communication;

1089   (3) adversely affect the right of an individual or any other person to exercise free speech,

1090   pursuant to the First Amendment to the United States Constitution, or to exercise another right

1091   provided for by law; or

1092   (4) apply to an entity's publication of entity-based member or employee contact

1093   information where such publication is intended to allow members of the public to contact such

1094   member or employee in the ordinary course of the entity's operations.

1095   (d) Personal information that is processed by a controller pursuant to an exemption under

1096   subsections (a) through (c) shall:

1097   (1) not be processed for any purpose other than those expressly listed in subsections (a)

1098   through (c), unless otherwise allowed by this chapter; and

1099   (2) notwithstanding anything in this section to the contrary, be processed: (i) in

1100   accordance with section 5 of this chapter; and (ii) subject to reasonable administrative, technical

1101   and physical measures to reduce reasonably foreseeable risks of harm to individuals.

1102   (e) If a controller processes personal information pursuant to an exemption in subsections

1103   (a) through (c) of this section, the controller bears the burden of demonstrating that such

1104   processing qualifies for the exemption and complies with the requirements of subsection (d).

1105   (f) A controller or processor that discloses personal information to a processor or third

1106   party in compliance with the requirements of this chapter shall not be in violation of this chapter

1107   if the recipient processes such personal information in violation of this chapter; provided,

1108   however, that at the time of disclosing the personal information, the disclosing controller or

1109   processor did not know or should not reasonably have known that the recipient intended to

1110   commit a violation.

1111   (g) A processor or third party receiving personal information from a controller or

1112   processor in compliance with the requirements of this chapter shall not be in violation of this

1113   chapter if the controller or processor from which it receives the personal information fails to

1114   comply with applicable obligations under this chapter; provided, however, that the processor or

1115   third party shall be liable for its own violations of this chapter.

1116   (h) If an individual has already consented to a controller's use, disclosure, or sale of their

1117   personal information to produce a physical item, such as a school yearbook, sections 8 through

1118   13 shall not apply to the controller's use, disclosure, or sale of the particular pieces of the

1119   individual's personal information for the production of that physical item; provided, however,

1120   that:

1121   (1) the controller has incurred significant expense in reliance on the individual's consent;

1122   (2) compliance with the individual's request to exercise the rights set forth in sections 8

1123   through 13 would not be commercially reasonable; and

1124   (3) the controller complies with the individual's request as soon as it is commercially

1125   reasonable to do so.

1126   Section 25. Powers of the Attorney General

1127   (a) Whenever the attorney general has reasonable cause to believe that an entity has

1128   engaged in, is engaging in, or is about to engage in a violation of this chapter, the attorney

1129   general may issue a civil investigative demand. The provisions of section 6 of chapter 93A of the

1130   General Laws shall apply mutatis mutandis to civil investigative demands issued under this

1131   chapter.

1132   (b) The attorney general shall have the authority to enforce the provisions of this chapter.

1133   A violation of this chapter, except as otherwise specified in section 26, shall not serve as the

1134   basis for or be subject to a private right of action under this chapter. Nothing in this chapter,

1135   except as otherwise specified in section 26, shall be construed as creating a new private right of

1136   action or serving as the basis for a private right of action that would not otherwise have had a

1137   basis under any other law but for the enactment of this chapter. This chapter neither relieves any

1138   party from any duties or obligations imposed, nor alters any independent rights that individuals

1139   have, under chapter 93A of the General Laws, other state or federal laws, the Massachusetts

1140   Constitution, or the United States Constitution.

1141   (c) Prior to initiating any civil action under this chapter, the attorney general shall provide

1142   an entity written notice identifying the specific provisions of this chapter that the attorney

1143   general alleges have been or are being violated.

1144   (d) (1) The entity shall have a period of 30 days in which to cure a violation after being

1145   provided notice by the attorney general. If within that time period the entity cures the noticed

1146   violation and provides the attorney general an express written statement that the alleged

1147   violations have been cured and that no such further violations shall occur, the attorney general

1148   shall initiate no action against the entity.

1149   (2) The cure period stipulated in paragraph (1) shall not apply when:

1150   (i) the court has previously issued a temporary restraining order, preliminary injunction,

1151   or permanent injunction or assessed civil penalties against the entity for a violation of: (A) this

1152   chapter; or (B) chapter 93A of the General Laws, provided that such violation occurs after the

1153   effective date of this section;

1154   (ii) the attorney general and the entity have previously reached a settlement that includes

1155   an admission by the entity that it has violated: (A) this chapter, not including any express written

1156   statement provided pursuant to paragraph (1); or (B) chapter 93A of the General Laws, provided

1157   that such admission occurs after the effective date of this section;

1158   (iii) the attorney general has clear and convincing evidence that the entity willfully and

1159   wantonly violated this chapter;

1160   (iv) the violation is a data broker's failure to register pursuant to section 20 of this

1161   chapter; or

1162   (v) the violation occurs more than twelve months after the effective date of this section

1163   and the violating entity is: (A) a large data holder; or (B) a data broker pursuant to paragraph (1)

1164   of the definition of data broker in section 2.

1165   (3) In its notice pursuant to subsection (c), the attorney general shall specify the length, if

1166   any, of the period in which the entity can cure the noticed violation.

1167   (e)(1) The attorney general may initiate a civil action against an entity in the name of the

1168   commonwealth or as parens patriae on behalf of individuals if the entity:

1169   (i) fails to cure a violation within 30 days after receipt of the attorney general's notice of

1170   the violation;

1171   (ii) breaches an express written statement provided to the attorney general pursuant to

1172   subsection (d); or

1173   (iii) is not eligible for a cure period pursuant to subsection (d).

1174   (2) The attorney general may seek:

1175   (i) civil penalties of up to 7,500 dollars for each violation under this chapter; and

1176   (ii) a temporary restraining order, preliminary injunction, or permanent injunction to

1177   restrain any violations of this chapter.

1178   (f) A data broker that fails to register as required by section 20 shall be subject to

1179   injunction and may be liable for civil penalties, fees and costs in a civil action brought on behalf

1180   of the commonwealth by the attorney general as follows:

1181   (1) a civil penalty of up to 500 dollars for each day, not to exceed a total of 100,000

1182   dollars for each year, that the data broker fails to register as required by section 20; and

1183   (2) fees equal to the fees that were due during the period the data broker failed to register.

1184   (g) The superior court shall have jurisdiction of actions brought under this section. Such

1185   actions may be brought in any county where a defendant resides or has its principal place of

1186   business or in which the violation occurred in whole or in part, or, with the consent of a

1187   defendant, in the superior court for Suffolk County.

1188   (h) In determining the overall amount of civil penalties to seek or assess against an entity,

1189   the attorney general or the court shall include, but not be limited to, the following in its

1190   consideration:

1191   (1) the size, scope and type of the entity;

1192   (2) the amount of resources available to the entity;

1193   (3) the amount and nature of personal information processed by the entity;

1194   (4) the number of violations;

1195   (5) the number of violations affecting children or minors;

1196   (6) the nature and severity of the violation;

1197   (7) the risks caused by the violation;

1198   (8) whether the entity's violation was an isolated instance or part of a pattern of

1199 violations and noncompliance with this chapter;

1200   (9) whether the entity is a data broker that did not register pursuant to section 20;

1201   (10) whether the violation was willful and not the result of error;

1202   (11) the length of time over which the violation occurred;

1203   (12) the precautions taken by the entity to prevent a violation;

1204   (13) the good faith cooperation of the entity with any investigations conducted by the

1205 attorney general pursuant to this section;

1206   (14) efforts undertaken by the entity to cure the violation; and

1207   (15) the entity's past violations of information privacy rules, regulations, codes,

1208 ordinances and laws in other jurisdictions.

1209   (i) Any entity that violates the terms of an injunction or other order issued under this

1210 section shall forfeit and pay a civil penalty of up to 10,000 dollars for each violation. For the

1211 purposes of this section, the court issuing such an injunction or order shall retain jurisdiction, and

1212   the cause shall be continued, and in such case the attorney general acting in the name of the

1213   commonwealth may petition for recovery of such civil penalty.

1214   (j) The attorney general may recover reasonable expenses, including attorney fees,

1215   incurred in investigating and preparing the case in any action initiated under this chapter.

1216   (k) If two or more entities are involved in the same processing that violates this chapter,

1217   the liability shall be allocated among the parties according to principles of comparative fault.

1218   (l) Notwithstanding any general or special law to the contrary, the court may require that

1219   the amount of a civil penalty imposed pursuant to this section exceeds the economic benefit

1220   realized by an entity for noncompliance.

1221   (m) If a series of steps or transactions were component parts of a single transaction

1222   intended to avoid the reach of this chapter, the attorney general and the court shall disregard the

1223   intermediate steps or transactions and consider everything one transaction for purposes of

1224   effectuating the purposes of this chapter.

1225   (n) Not later than 30 days after the end of each calendar year, the attorney general shall

1226   publish a public, easily accessible report that provides, for that calendar year, the following

1227   information:

1228   (1) the number of written notices issued pursuant to subsection (c) and the number of

1229   entities that received such notices;

1230   (2) examples of alleged violations that have been cured by an entity pursuant to

1231   subsection (d); and

1232   (3) categories of violations of this chapter and the number of violations per category.

1233   (o) The attorney general shall receive and may investigate sworn complaints from an

1234   individual or other natural person that an entity has engaged in, is engaging in, or is about to

1235   engage in any violation of this chapter.

1236   (p) The attorney general shall maintain the following internet web pages:

1237   (1) a web page that includes an online mechanism through which any individual or other

1238   natural person may contact the attorney general to submit a sworn complaint;

1239   (2) a web page that enables data brokers to register pursuant to section 20; and

1240   (3) a web page that:

1241   (i) makes publicly accessible the information provided by each data broker pursuant to

1242   section 20; provided, however, that the information shall be disaggregated by data broker; and

1243   (ii) includes a link and mechanism, if feasible, by which an individual may: (A) pursuant

1244   to section 8, opt out of the processing of the individual's personal information by all registered

1245   data brokers for the purposes of the sale of such information or for targeted cross-contextual

1246   advertising; and (B) pursuant to section 11, request that all registered data brokers delete any

1247   personal information processed about the individual.

1248   (q) The attorney general shall promote public awareness and understanding of the risks,

1249   rules, responsibilities, safeguards and rights in relation to the processing of personal information,

1250   including, but not limited to, the rights of children and minors with respect to their own

1251   information. The attorney general shall provide guidance to individuals regarding what to do if

1252   they believe their rights under this chapter have been violated.

1253   (r) The attorney general shall create and make publicly accessible the following

1254   templates:

1255   (1) a template privacy policy that meets the requirements of section 7;

1256   (2) a template contract between a controller and a processor that meets the requirements

1257   of section 19; and

1258   (3) a template risk assessment that meets the requirements of section 21.

1259   (s) The attorney general shall seek to collaborate with entities responsible for enforcing

1260   personal information privacy laws in other jurisdictions. The attorney general shall have the

1261   power to determine, pursuant to section 28, whether the provisions of a personal information

1262   privacy law in another jurisdiction are equally or more protective of personal information than

1263   the provisions of this chapter.

1264   (t) The attorney general shall establish a mechanism pursuant to which an entity that

1265   processes the personal information of one or more individuals but does not meet the applicability

1266   criteria set forth in subsection (b) of section 3 may voluntarily certify that it is fully in

1267   compliance with, and agrees to be bound by, this chapter. The attorney general shall make a list

1268   of those entities available to the public.

1269   (u) The attorney general shall adopt regulations for the purposes of carrying out this

1270   chapter, including, but not limited to, the following areas:

1271   (1) supplementing any of the definitions used in this chapter or adding in new definitions

1272   for terms that are used but not otherwise defined in this chapter, in order to address changes in

1273   technology, data collection, obstacles to implementation and privacy concerns;

1274   (2) ensuring that the notices and information that controllers are required to provide

1275   pursuant to section 7 are:

1276   (i) provided in a manner that may be easily understood by the average individual;

1277   (ii) accessible to individuals with disabilities; and

1278   (iii) available in the language primarily used to interact with the individual;

1279   (3) detailing the requirements and technical specifications for a platform, technology or

1280   mechanism that sends an opt-out preference signal indicating an individual's intent to opt out of

1281   the processing of such individual's personal information for one or more of the purposes

1282   specified in subsection (a) of section 8; provided, however that the requirements and technical

1283   specifications shall be updated from time to time to reflect the means by which individuals

1284   interact with controllers; and provided further, that any such platform, technology or mechanism

1285   shall:

1286   (i) not unfairly disadvantage another controller;

1287   (ii) clearly represent the individual's affirmative, freely-given and unambiguous intent to

1288   opt out pursuant to subsection (a) of section 8 and be free of default settings constraining or

1289   presupposing that intent;

1290   (iii) be consumer-friendly, clearly described and easy to use by the average individual;

1291   (iv) be as consistent as possible with any other similar platform, technology or

1292   mechanism required by any federal or state law or regulation; and

1293   (v) enable the controller to accurately determine if the mechanism represents a legitimate

1294   opt-out request pursuant to section 8; and

1295   (4) supplementing or revising the list of industry recognized cybersecurity frameworks

1296   specified in paragraphs (1) and (2) of subsection (d) of section 26, in order to address changes in

1297   technology, data collection, obstacles to implementation, best practices with respect to

1298   cybersecurity controls and privacy concerns.

1299   (v) The attorney general shall conduct research and monitor relevant developments

1300   relating to the protection of personal information, the development of information and

1301   communication technologies and commercial practices and the enactment and implementation of

1302   privacy laws by the federal government or other states, territories or countries. Specific topics for

1303   research shall include, but are not limited to, the following areas:

1304   (1) the available best methods for: (i) individuals to exercise the rights set forth in

1305   sections 8 through 13; and (ii) entities to conspicuously and clearly disclose how to exercise such

1306   rights;

1307   (2) automated decision-making technologies;

1308   (3) eye-tracking technology and targeted advertising based on information collected

1309   through eye-tracking technology;

1310   (4) financial incentive programs offered by controllers for the processing of personal

1311   information;

1312   (5) the data broker industry, including data brokers that have registered pursuant to

1313   section 20;

1314   (6) the effectiveness of allowing an individual to designate an authorized agent to

1315   exercise a right on their behalf pursuant to section 8; and

1316   (7) whether to change or eliminate the cure period established in subsection (d) of section

1317   25.

1318   (w) Every twelve months, the attorney general shall provide a full written report to the

1319   joint committee on advanced information technology, the internet and cybersecurity. The report

1320   shall summarize the attorney general's work pursuant to this section and detail the attorney

1321   general's research and any recommendations with respect to privacy-related legislation. The first

1322   such report shall be submitted 12 months after the effective date of this subsection.

1323   (x) The monetary amounts referred to in this chapter shall be indexed biennially for

1324   inflation by the attorney general, who, not later than December 31 of each even numbered year,

1325   shall calculate and publish such indexed amounts, using the federal consumer price index for the

1326   Boston statistical area and rounding to the nearest dollar.

1327   Section 26. Private Right of Action and Safe Harbor

1328   (a) For the purposes of this section, except for the purposes of determining whether this

1329   section applies to a given controller, the terms "breach of security" and "personal information"

1330   shall have the same meanings as such terms are defined in section 1 of chapter 93H of the

1331   General Laws.

1332   (b) Any individual whose personal information is subject to a breach of security as a

1333   result of a controller's failure to implement and maintain reasonable cybersecurity controls may

1334   institute a civil action for any of the following:

1335   (1) damages from the controller in an amount up to 500 dollars per individual per

1336   incident or actual damages, whichever is greater;

1337   (2) injunctive or declaratory relief; or

1338   (3) any other relief the court deems proper.

1339   (c) In determining the amount of statutory damages against the controller, the court shall

1340   consider any one or more of the relevant circumstances presented by any of the parties to the

1341   case, including, but not limited to, the criteria stipulated in paragraphs (1) through (15) of

1342   subsection (h) of section 25.

1343   (d) In any cause of action founded in tort that is brought pursuant to this section and that

1344   alleges that the controller's failure to implement reasonable cybersecurity controls resulted in a

1345   breach of security concerning personal information, the court shall not assess punitive damages

1346   against a controller if such controller created, maintained and complied with a written

1347   cybersecurity program that contains administrative, technical and physical safeguards for the

1348   protection of personal information and that conforms to an industry recognized cybersecurity

1349   framework; provided, however, that the controller designed and implemented its cybersecurity

1350   program in accordance with the regulations adopted pursuant to chapter 93H of the General

1351   Laws; and provided further, that:

1352   (1) such cybersecurity program conforms to the current version of or any combination of

1353   the current versions of:

1354   (i) the "Framework for Improving Critical Infrastructure Cybersecurity" published by the

1355   National Institute of Standards and Technology;

1356   (ii) the National Institute of Standards and Technology's special publication 800-171;

1357   (iii) the National Institute of Standards and Technology's special publications 800-53 and

1358   800-53a;

1359   (iv) the Federal Risk and Authorization Management Program's "FedRAMP Security

1360   Assessment Framework";

1361   (v) the Center for Internet Security's "Center for Internet Security Critical Security

1362   Controls for Effective Cyber Defense"; or

1363   (vi) the "ISO/IEC 27000-series" information security standards published by the

1364   International Organization for Standardization and the International Electrotechnical

1365   Commission; or

1366   (2) such program complies with the current version of the "Payment Card Industry Data

1367   Security Standard" and the current version of another applicable industry recognized

1368   cybersecurity framework described in paragraph (1).

1369   (e) When a revision to a document listed in paragraphs (1) or (2) of subsection (d) is

1370   published, a controller whose cybersecurity program conforms to a prior version of that

1371   document shall be said to conform to the current version of that document if the controller

1372   conforms to such revision not later than six months after the publication date of the revision.

1373   (f) The scale and scope of a controller's cybersecurity program shall be based on:

1374   (1) the size, scope and type of the controller;

1375   (2) the amount of resources available to the controller;

1376   (3) the amount and nature of personal information processed by the controller; and

1377   (4) the need for upholding security, integrity and confidentiality with respect to the

1378   personal information processed by the controller.

1379   (g) Subsection (d) shall not apply if the controller's failure to implement reasonable

1380   cybersecurity controls was the result of gross negligence or willful or wanton conduct.

1381   (h) Nothing in this section shall limit the authority of the attorney general to initiate

1382   actions pursuant to:

1383   (1) section 25 of this chapter;

1384   (2) chapter 93A or 93H of the General Laws; or

1385   (3) any other general law.

1386   (i) The cause of action established by this section shall apply only to violations as defined

1387   in this section.

1388   Section 27. Massachusetts Privacy Fund

1389   (a) There shall be established upon the books of the commonwealth a separate special

1390   fund to be known as the Massachusetts Privacy Fund.

1391   (b) All civil penalties, expenses, attorney fees and registration fees collected pursuant to

1392   sections 20 and 25 shall be paid into the state treasury and credited to the Massachusetts Privacy

1393   Fund. Interest earned on moneys in the fund shall remain in the fund and be credited to it. Any

1394   moneys remaining in the fund, including interest thereon, at the end of each fiscal year shall

1395   remain in the fund and not revert to the general fund.

1396   (c) The attorney general shall have discretion to allocate the proceeds of any settlement of

1397   a civil action pursuant to this chapter to:

1398   (1) the Massachusetts Privacy Fund;

1399   (2) the general fund; or

1400   (3) where possible, directly to individuals impacted by the violation of the chapter.

1401   (d) Moneys in the Massachusetts Privacy Fund shall be used to support the work of the

1402   attorney general pursuant to section 25. Moneys in the fund shall be subject to appropriation and

1403   shall not be used to supplant general fund appropriations to the attorney general.

1404   Section 28. Reciprocity and Interoperability

1405   (a) A controller or processor shall be in compliance with provisions of this chapter if:

1406   (1) it complies with comparable provisions of a personal information privacy law in

1407   another jurisdiction;

1408   (2) the controller or processor applies the provisions of that law to its processing

1409   activities concerning individuals; and

1410   (3) the attorney general determines that the provisions of that law in the other jurisdiction

1411   are equally or more protective of personal information than the provisions of this chapter.

1412   (b) The attorney general may charge a fee to a controller or processor that asserts

1413   compliance with a comparable law under subsection (a); provided, however, that the fee shall

1414   reflect costs reasonably expected to be incurred by the attorney general to determine whether the

1415   provisions of such law are equally or more protective than the provisions of this chapter.

1416   Section 29. Severability

1417   (a) The provisions of this chapter are severable. If any provision of this chapter, or the

1418   application of any provision of this chapter, is held invalid, the remaining provisions, or

1419   applications of provisions, shall remain in full force and not be affected.

1420   (b) If a court were to find in a final, unreviewable judgment that the exclusion of one or

1421   more entities or activities from the applicability of this chapter renders the chapter

1422   unconstitutional, those exceptions shall be rendered null and invalid and the exemption shall not

1423   continue.

1424   Section 30. Implementation for Nonprofits and Institutions of Higher Education

1425   This chapter shall apply to nonprofit organizations and institutions of higher education.

1426   SECTION 2. Chapter 93M of the General Laws shall take effect 18 months after the

1427   passage of this act; provided, however, that:

1428   (1) section 2 and subsections (p) through (w) of section 25 of the chapter shall take effect

1429   upon the passage of this act; and

1430   (2) section 30 of the chapter shall take effect 30 months after the passage of this act.