

SENATE NO. 160

AN ACT ESTABLISHING THE PROTECTION OF PERSONAL INFORMATION PROTECTION

*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. Chapter 24A of the General Laws is hereby amended by adding the following 3 sections:-

2 Section 6. In the course of administering chapter 66B, the office shall:

3 (1) engage in a public awareness campaign publicizing a data subject's rights under said
4 chapter 66B, including the posting of the new law on the office's webpage and undertaking any other
5 methods reasonably calculated to inform a data subject of his new legal rights under said chapter 66B;

6 (2) inform a commercial entity doing business in the commonwealth of it's duties under
7 said chapter 66B; and

8 (3) establish a procedure by which a data subject can easily and promptly register a
9 complaint about a commercial entity's or third party's failure to comply with said chapter 66B.

10 Section 7. (a) If the office finds that a commercial entity or third party violated chapter 66B, it
11 shall levy a fine of not more than \$5,000 per violation. The office shall determine the amount of this
12 fine by considering:

13 (1) the egregiousness of the violation;

14 (2) the party's past violations of chapter 66B;

15 (3) the threat that the violation poses to the integrity and security of a data subject's
16 personal data; and

17 (4) the effect the violation has on this act's ability to ensure a data subject's privacy.

18 (b) The office may refer any perceived material violation of this act to the attorney
19 general's office for further investigation.

20 Section 8. The office may promulgate regulations to assist in the administration of its duties
21 chapter 66B which shall be promulgate pursuant to the procedures for regulations not requiring
22 hearings as set forth in section 3 of chapter 30A.

23 SECTION 2. Title X of the General Laws is hereby amended by striking out the title and
24 inserting in place thereof the following title:-

25 PUBLIC RECORDS AND PERSONAL DATA.

26 SECTION 3. The General Laws are hereby amended by inserting after chapter 66A the
27 following chapter:-

28 CHAPTER 66B.

29 PERSONAL INFORMATION PROTECTION.

30 Section 1. As used in this chapter, the following words shall have the following meanings
31 unless the context clearly requires otherwise:

- 32 (a) “Commercial entity”, an entity that collects information in the course of its commercial
33 dealings, including, but not limited to associations, businesses, charitable organizations, clubs,
34 government entities, professional practices and unions.
- 35 (b) “Data collection program”, a program by which a commercial entity collects personal data and
36 creates a system of records so that personal data can be retrieved by using the data subject’s
37 identity.
- 38 (c) “Data subject”, an individual to whom personal data refers; provided, however, that “data
39 subject” shall not include corporations, corporate trusts, partnerships, limited partnerships,
40 trusts or other similar entities.
- 41 (d) “Office”, the officer of consumer affairs and business regulation.
- 42 (e) “Opt out”, to cease participation in a data collection program without incurring any
43 unreasonable discrimination or disruption in service and receiving the same quality of service
44 as before.
- 45 (f) “Personal data”, information that a commercial entity or third party can associate with a
46 particular individual because the information contains a name, description, unique number or
47 identifying mark, including, but not limited to, zip code, phone number, address or social
48 security number.
- 49 (g) “Processor”, the third party that obtains personal data to perform a contracted business
50 function for a commercial entity, including, but not limited to, processing a payment,
51 administering a warranty and evaluating customer credit.
- 52 (h) “Public records”, all books, papers, maps, photographs, recorded tapes, financial statements,
53 statistical tabulations, or other documentary materials or data, regardless of physical form or
54 characteristics, made or received by an officer or employee of an agency, executive office,

55 department, board, commission, bureau, division or authority of the commonwealth, or of any
56 political subdivision thereof, or of any authority established by the general court to serve a
57 public purpose; provided, however, that “public records” shall not include the exceptions to
58 that term as set forth in clause Twenty-sixth of section 7 of chapter 4.

59 (i) “Third-party”, an entity that obtains personal data from a commercial entity, including, but not
60 limited to, an association, business, charitable organization, club, governmental body,
61 institution, professional practice and union.

62 Section 2. A data subject may opt out of a commercial entity’s data collection program at any time
63 and without charge.

64 Section 3. A data subject who believes a commercial entity or third party has violated this chapter
65 may seek redress by any of the following: (i) the commercial entity’s grievance procedures as
66 established pursuant to clause (6) of subsection (b) of section 4; (ii) the office’s complaint registering
67 procedure established in subsection (c) of section 6 of chapter 24A; or (iii) an independent cause of
68 action in the district or superior court department of the trial court.

69 Section 4. (a) A commercial entity that collects personal data shall, at the point of data collection,
70 conspicuously post a written privacy policy that complies with this chapter which shall clearly and
71 simply:

- 72 (1) identify the purposes for which the commercial entity collects personal data;
- 73 (2) limit itself to only collecting personal data necessary to serve the purposes the
74 commercial entity has set forth pursuant to clause (1);
- 75 (3) commit itself to retaining personal data for only as long as necessary to serve the
76 purposes the commercial entity as set forth pursuant to clause (1);
- 77 (4) detail the circumstances in which the commercial entity may distribute personal

- 78 data to third parties;
- 79 (5) detail how the commercial entity ensures the accuracy and security of personal data;
- 80 (6) state that, upon a data subject's request, the commercial entity shall allow the data
81 subject access to the commercial entity's store of that data subject's personal data;
- 82 (7) establish a method for a data subject to correct erroneous information;
- 83 (8) inform a data subject, in conspicuous and bold font, that he may opt out of the
84 commercial entity's data collection program at any time and free of charge;
- 85 (9) detail the procedure by which a data subject may opt out of the data collection
86 program; and
- 87 (10) provide a data subject with further resources that provide information about more
88 specific aspects of the commercial entity's information collection policies and
89 procedures.

90 (b) A commercial entity that collects personal data shall:

- 91 (1) designate an individual immediately responsible for ensuring compliance with this
92 chapter;
- 93 (2) inform all individuals who have a role in the design, development, operation or
94 maintenance of the data collection program of: (i) the requirements of this chapter;
95 and (ii) each regulation the promulgated by the office pursuant to section 8 of
96 chapter 24A;
- 97 (3) limit its use of personal data to those uses necessary to serve the purposes the
98 commercial entity has set forth pursuant to subsection (a);
- 99 (4) establish a procedure by which a data subject may opt out of a commercial entity's
100 data collection program at any time and free of charge and a commercial entity shall

101 ensure that this procedure does not require the data subject to perform overly-
102 burdensome tasks to opt out of the data collection program;
103 (5) take all reasonable steps to ensure the security and accuracy of the personal data it
104 collects and retains; provided, however, that a commercial entity shall take
105 reasonable precautions to protect personal data from fire, theft, flood, natural
106 disaster, unintended dissemination or other physical threat; and
107 (6) establish a reasonably simple procedure by which a data subject can file a grievance
108 with the individual responsible for ensuring the commercial entity's compliance
109 with this chapter.

110 (c) A commercial entity that collects personal data shall not obtain a public record pursuant to
111 its data collection program for the purpose of obtaining the personal data that the public record
112 contains.

113 (d) Notwithstanding any general or special law to the contrary, a commercial entity that collects
114 personal data shall not divulge such data to a third party that is not acting as a processor.

115 Section 5. A processor who obtains personal data from a commercial entity shall only keep the
116 personal data for as long as it reasonably takes to accomplish its processing task.

117 Section 6. To assist the office in enforcing this chapter, a trial court:-

- 118 (1) shall recognize a violation of this act as a per se deceptive trade practice under chapter 93A;
119 (2) may impose such equitable relief as it finds reasonably necessary to accomplish the objectives
120 of this chapter, including an injunction and specific performance;
121 (3) shall not preclude other grounds for recovery that a data subject may have against a
122 commercial entity or third party;
123 (4) shall resolve all ambiguity in favor of protecting a consumer's privacy; and

124 (5) shall not recognize a cause of action under this chapter after 3 years from the date of an alleged
125 violation.

126 SECTION 4. Section 1 of chapter 161A of the General Laws, as appearing in the 2002 Official
127 Edition, is hereby amended by inserting after the definition of “Capital investment program” the
128 following 2 definitions:-

129 “Data collection program”, a program by which a commercial entity collects personal data and
130 creates a system of records so that personal data can be retrieved by using the data subject’s identity.

131 “Data subject”, an individual to whom personal data refers; provided, however, that “data
132 subject” shall not include a corporation, corporate trust, partnership, limited partnership, trust, or other
133 similar entity.

134 SECTION 5. Said section 1 of said chapter 161, as so appearing, is hereby further amended by
135 inserting after the definition of “Passenger miles” the following 2 definitions:-

136 “Personal data”, information that a commercial entity or third party can associate with a
137 particular individual because the information contains a name, description, unique number or
138 identifying mark, including, but not limited to, zip code, phone number, address or social security
139 number.

140 “Processor”, the third party that obtains personal data to perform a contracted business function
141 for a commercial entity, including, but not limited to, processing a payment, administering a warranty
142 and evaluating customer credit.

143 SECTION 6. Said section 1 of said chapter 161, as so appearing, is hereby further amended by
144 inserting after the definition of “Rider” the following definition:-

145 “Ridership data”, information that details the time and location at which a rider utilized the
146 authority’s services.

147 SECTION 7. Said section 1 of said chapter 161, as so appearing, is hereby further amended by
148 adding the following definition:-

149 “Third-party”, an entity that obtains personal data from a commercial entity, including, but not
150 limited to, an association, business, charitable organization, club, governmental body, institution,
151 professional practice and union.

152 SECTION 8. Said chapter 161A of the General Laws is hereby amended by adding the following 2
153 sections:-

154 Section 49. Personal data collected by the authority shall not be linked, or capable of becoming
155 linked, to ridership data for a passenger.

156 Section 50. Notwithstanding any general or special law to the contrary, the authority shall not share
157 personal data with a third party that is serving as a processor.

158 SECTION 9. Within 120 days after the effective date of this act, a commercial entity shall mail a copy
159 of the privacy policy the commercial entity shall post pursuant to subsection (a) of section 4 to a data
160 subject for which the commercial entity has a physical or electronic mailing address.

161 SECTION 10. The director of consumer affairs and business regulation shall monitor and evaluate the
162 enforcement and effectiveness of chapter 66B of the General Laws. The director shall file a report
163 with the appropriate committees of the general court concerning it’s their evaluation not later than 2
164 years after the effective date of said chapter 66B.