



SPONSOR: Rep. Griffith & Rep. Matthews & Rep. Baumbach &
Rep. Dorsey Walker & Sen. Hansen & Sen. Gay
Reps. Lambert, Morrison; Sen. Ennis

HOUSE OF REPRESENTATIVES
151st GENERAL ASSEMBLY

HOUSE BILL NO. 262

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO DATA BROKERS AND CONSUMER PROTECTION.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE (Three-fifths of all members elected to each house thereof concurring therein):

1 Section 1. Amend Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as
2 shown by underline as follows:

3 Chapter 12D. Protection of Personal Information.

4 § 12D-101. Definitions.

5 For purposes of this chapter, the following definitions shall apply:

6 (1)a. “Brokered personal information” means one or more of the following computerized data elements about
7 a consumer, if categorized or organized for dissemination to third parties:

8 (i) name;

9 (ii) address;

10 (iii) date of birth;

11 (iv) place of birth;

12 (v) mother's maiden name;

13 (vi) unique biometric data generated from measurements or technical analysis of human body
14 characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a
15 fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric
16 data;

17 (vii) name or address of a member of the consumer's immediate family or household;

18 (viii) Social Security number or other government-issued identification number; or

19 (ix) other information that, alone or in combination with the other information sold or licensed,
20 would allow a reasonable person to identify the consumer with reasonable certainty.

21 b. “Brokered personal information” does not include publicly available information to the extent that it is
22 related to a consumer’s business or profession.

23 (2) “Business” means a commercial entity, including a sole proprietorship, partnership, corporation,
24 association, limited liability company, or other group, however organized and whether or not organized to operate at a
25 profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the
26 laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a
27 financial institution.

28 (3) “Consumer” means an individual residing in this State.

29 (4)a. “Data broker” means a business that both (i) knowingly maintains or collects the brokered personal
30 information of at least 500 consumers and (ii) either sells or licenses such information to one or more independently
31 operated businesses. The term “data broker” includes, but is not limited to, data collectors and third-party data brokers.
32 A business may be both a data collector and a third-party data broker depending on its activities.

33 b. “Data collector” means a data broker that initially collects personal data from one or more consumers
34 through a transaction or observation.

35 b. “Third-party data broker” means a data broker that receives the brokered personal information of one
36 or more consumers with whom the data broker does not have a direct relationship (e.g., employee, contractor,
37 agent, investor, donor, customer, client, subscriber, user, or other similar relationship in which the consumer
38 would be aware that the data broker received the consumer’s personal information directly from the consumer).

39 c. The following activities conducted by a business, and the collection and sale or licensing of brokered
40 personal information incidental to conducting these activities, do not qualify the business as a data broker:

41 1. Providing 411 directory assistance or directory information services, including name, address, and
42 telephone number, on behalf of or as a function of a telecommunications carrier;

43 2. Providing publicly available information related to a consumer's business or profession; or

44 3. Providing publicly available information via real-time or near-real-time alert services for health or
45 safety purposes; or

46 4. Providing brokered personal information of an individual to an employer, potential employer,
47 government agency, or contractual counterparty of the individual, with the written authorization of such
48 individual in connection with a background check of such individual.

49 5. Providing brokered personal information where authorized by 21 Del. C. §305.

50 d. The phrase “sells or licenses” does not include:

51 1. A one-time or occasional sale of assets of a business as part of a transfer of control of those assets
52 that is not part of the ordinary conduct of the business; or

53 2. A license of data that is both incidental to a contract the business has with a third-party service
54 provider and necessary for such third-party service provider of the business to accomplish the purpose of such
55 contract, provided that the third-party service provider's permitted uses of the licensed data is limited to
56 fulfilling its contractual obligations to the business; or

57 3. The disclosure or transfer of brokered personal information pursuant to the terms of a subpoena, a
58 court order, a regulation, a statute, a response to a discovery request, or other legal obligation.

59 (5)a. "Data broker security breach" means, with respect to brokered personal information, a "breach of
60 security" as set forth in § 12B-101(1) of Chapter 12B of this title.

61 b. In determining whether brokered personal information was acquired or is reasonably believed to have
62 been accessed or obtained by a person without valid authorization, a data broker shall consider all relevant factors,
63 including but not limited to the following factors:

64 1. Indications that the brokered personal information is in the physical possession and control of a
65 person without valid authorization, such as a lost or stolen computer or other device containing brokered
66 personal information;

67 2. Indications that the brokered personal information was accessed, downloaded, or copied;

68 3. Indications that an unauthorized person used the brokered personal information, such as the
69 opening of fraudulent accounts or reports of identity theft; and

70 4. Indications that the brokered personal information has been made public.

71 (6) "Encryption" means the use of an algorithmic process to transform data into a form in which the data is
72 rendered unreadable or unusable without use of a confidential process or key.

73 (7) "License" means a grant of access to, or distribution of, data by one person to another in exchange for
74 consideration. A license does not include use of data for the sole benefit of the data provider if the data provider
75 maintains control over the use of the data.

76 (8) "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is
77 recorded or preserved, regardless of physical form or characteristics.

78 § 12D-102. Prohibitions on the acquisition and dissemination of brokered personal information.

79 (a) A person shall not acquire brokered personal information through deception, false representations, or other
80 fraudulent means, including on the basis of misrepresentations or material omissions about the data collector's use of the
81 brokered personal information.

82 (b) A person shall not acquire or use brokered personal information for the purpose of any of the following:

83 (1) Stalking or harassing another person.

84 (2) Committing a fraud, including identity theft, financial fraud, or e-mail fraud.

85 (3) Engaging in unlawful discrimination, including employment discrimination and housing discrimination.

86 (c) A data broker shall not provide for consideration, whether by sale, license, or other exchange, to another person
87 brokered personal information where that data broker knows or reasonably should know that such brokered personal
88 information was acquired in a manner prohibited by §12D-102(a), above.

89 (d) A data broker shall not provide for consideration, whether by sale, license, or other exchange, to another
90 person brokered personal information where that data broker knows or reasonably should know that such brokered personal
91 information will be used for any of the purposes set forth in §12D-102(b), above.

92 (e) A violation of subsections (a), (b), (c), or (d) of this section shall be deemed an unlawful practice under § 2513
93 of this title and a violation of subchapter II of Chapter 25 of this title.

94 § 12D-103. Annual registration of data brokers.

95 (a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as
96 provided in § 12D-101 of this title, a data broker shall do all of the following:

97 (1) Register with the Consumer Protection Unit of the Department of Justice.

98 (2) Pay a registration fee calculated based on the activity of the data broker in the year immediately preceding
99 the date of registration, as follows:

100 a. For a data broker who sold or licensed the brokered personal information of not more than 5,000
101 consumers and engaged in not more than 5 such sale or license transactions during the relevant year, the
102 registration fee is \$10.

103 b. For a data broker who is not eligible for the fee under sub-paragraph (a)(2)a., above, and who sold or
104 licensed the brokered personal information of not more than 200,000 consumers, the registration fee is equal to the
105 multiple of the number of consumers times \$0.0025, rounded up to the nearest \$10.

106 c. For a data broker who sold or licensed the brokered personal information of more than 200,000
107 consumers, the registration fee is \$500.

108 d. For registration fees due in each year after 2022, the calculations in paragraph (a)(2) of this section
109 shall be increased by multiplying the registration fee calculated pursuant to paragraphs (a)(2)b. and (a)(2)c. of this
110 section by the cumulative change in the national consumer price index from January 1, 2021 to January 1 in the
111 year in which the registration fee is due. The registration fee due pursuant to paragraph (a)(2)a. is not subject to
112 such increase.

113 (3) In an electronic form designated by the Director of Consumer Protection, provide all of the following
114 information, accompanied by a certification of the accuracy of such information:

115 a. The name and primary physical, e-mail, and Internet addresses of the data broker and links to all
116 privacy policies issued by the data broker that are applicable to the brokered personal information that it collects or
117 maintains.

118 b. If the data broker permits a consumer to opt out of the data broker's collection of brokered personal
119 information, opt out of the inclusion, use, or processing of the consumer's information in the data broker's
120 databases, or opt out of certain sales of data about the consumer:

121 1. The method for requesting an opt-out, including, as applicable, each of the following:

122 A. a direct weblink to an opt-out form.

123 B. an email address to which opt out requests can be made

124 C. a phone number to which opt-out requests can be made

125 D. a physical address to which opt-out requests can be emailed.

126 2. If the opt-out applies to only certain activities or sales, which ones.

127 3. Whether the data broker permits a consumer to authorize a third party to perform the opt-out on
128 the consumer's behalf.

129 c. A statement specifying the data collection, databases, or sales activities from which the data broker
130 does not offer the consumer any ability to opt out.

131 d. A description of the data broker's process for verifying the purchasers of its brokered personal
132 information, along with such purchasers' compliance with relevant privacy policies and representations, including
133 any purchaser credentialing process.

134 e. The number of data broker security breaches that the data broker has experienced during the prior 3
135 years, and if known, the total number of consumers affected by the breaches.

136 f. Where the data broker has actual knowledge that it possesses the brokered personal information of
137 minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies
138 that are applicable to the brokered personal information of minors.

139 g. Answers in the provided form to each of the following questions:

140 Question: Are you a data collector? Answer Choices: yes; no.

141 Question: Are you a third-party data broker? Answer Choices: yes; no.

142 Question: Identify the six-digit NAICS (North American Industry Classification System) Code for
143 your business: Answer Choice: [6-digit Numeric Response]

144 Question: Which of the following categories of consumer data do you collect directly from
145 consumers and from consumers' devices? Answer Choices (indicate all that apply): (0) none; (1) name,
146 telephone, or contact information; (2) demographic information, such as age, gender, gender-identity; (2a)
147 data related to the assignment of a consumer to predicted demographic categories; (3) race, nationality,
148 ethnicity, or sexual preference data; (4) geolocation data; (5) financial account data; (6) income or wealth
149 data; (7) employment data; (8) biometric data; (9) device-based user activity data; (10) health data; (11)
150 genetic data; (12) social security number or other government-issued identification number; (13) internet
151 browsing data; (14) information on a consumer's purchasing history; (15) date of birth; (15) criminal history;
152 (16) information on a consumer's status as a victim of a crime; (17) other

153 Question: Which of the following categories of consumer data do you purchase or license from other
154 data brokers? Answer Choices [SAME]

155 Question: Which of the following categories of consumer data do you sell or license to other third
156 parties? Answer Choices [SAME]

157 Question: To which of the following categories of third party do you sell or license such consumer
158 data? Answer Choices (indicate all that apply): (0) none; (1) financial institutions; (2) insurance providers; (3)
159 healthcare providers; (3) non-profit organizations; (4) law enforcement agencies; (5) non-law enforcement
160 governmental agencies or subdivisions; (6) advertising platforms; (7) lead generators; (8) charitable
161 solicitors; (9) non-US based businesses; (10) non-US governments; (11) third-party data brokers; (12) other.

162 Question: Do you limit the use of brokered personal information by a purchaser or licensee receiving
163 brokered personal information from you? Answer Choices (indicate all that apply): (1) Yes, we require all
164 recipients to comply with our privacy policies that are applicable to such information when in our control; (2)

165 Yes, we contractually limit use to those purposes set forth in our contract; (3) Yes, we prohibit resale; (4) Yes,
166 we limit uses in ways other than those methods listed in answer choices (1), (2) and (3); (5) No.

167 Question: If you answered “yes” to the preceding question, what steps do you take to ensure the
168 purchaser’s or licensee’s compliance with those limitations? Answer Choices (indicate all that apply): (1)
169 maintain a right to audit or inspect the purchaser or licensee; (2) require and receive periodic reports on
170 compliance from the purchaser or licensee; (3) conduct periodic not-for-cause audits or inspections of the
171 purchaser or licensee; (4) conduct for-cause audits or inspections of the purchaser or licensee; (5) other.

172 Question: How many complaints or reports have you received about the use, sale, licensing, or other
173 disclosure of consumers brokered personal information in a manner incompatible with its collection?

174 Question: Have you received any reports from persons to whom you sold or licensed brokered
175 personal information of any violation of the terms of such sale or license?

176 Question: Have you terminated the sale or license of any brokered personal information based in
177 whole or in part on any violation of the terms of such sale or license?

178 Question: For any brokered personal information that you purchase or license from a third party, do
179 you comply with the privacy policies of the third party? Answer Choices: (1) Yes; (2) No.

180 h. On an annual basis by September 1 in the year preceding the year in which a registration is due, the
181 Director of Consumer Protection may add and remove questions and answer choices to the questions set forth in
182 paragraph (a)(3)g. of this section as the Director determines to be appropriate in light of the evolving nature of the
183 data brokerage industry.

184 i. Any additional information or explanation the data broker chooses to provide concerning its data
185 collection practices.

186 (b) A data broker that fails to register pursuant to subsection (a) of this section is liable to the State for all of the
187 following:

188 (1) A civil penalty of \$50 for each day, not to exceed a total of \$10,000 for each year, it fails to register
189 pursuant to this section;

190 (2) An amount equal to the fees due under this section during the period it failed to register pursuant to this
191 section; and

192 (3) Other penalties imposed by law.

193 (c) A data broker that includes information it knows or reasonably should know to be false in a registration
194 submitted pursuant to subsection (a) of this section is liable to the State for all of the following:

195 (1) A civil penalty of \$50 for each day, not to exceed a total of \$10,000 for each year, its registration included
196 such false information;

197 (2) An amount equal to the fees due under this section during the period its registration included such false
198 information, which shall be in addition to any fees already paid; and

199 (3) Other penalties imposed by law.

200 (d) Nothing in this section shall limit the applicability of other consumer protection laws to the conduct of a data
201 broker.

202 § 12D-104. Data broker duty to protect personal information.

203 (a) A data broker shall develop, implement, and maintain a comprehensive information security program that is
204 written in more readily accessible parts and contains administrative, technical, and physical safeguards that are reasonably
205 designed to achieve the following objectives:

206 (1) Ensuring the security and confidentiality of brokered personal information.

207 (2) Protecting against any anticipated threats or hazards to the security or integrity of brokered personal
208 information, including internal and external threats or hazards.

209 (3) Protecting against the unauthorized acquisition of, or access to, brokered personal information.

210 (b) In determining whether a comprehensive information security program required by this section is reasonably
211 designed, the following factors shall be considered:

212 (1) The size, scope, and type of the data broker's business.

213 (2) The amount of resources available to the data broker relative to the cost to the data broker to implement
214 and maintain the security procedures.

215 (3) The amount of brokered personal information maintained by the data broker.

216 (4) The sensitivity of the brokered personal information to be protected.

217 (5) The data broker's information security program and practices as a whole.

218 (c) A data broker's comprehensive information security program shall be deemed to be reasonably designed for
219 purposes of subsection (a) of this section if any of the following are true:

220 (1) The program conforms to the standards or framework of a nationally- or internationally-recognized
221 standards-setting organization in the field of cybersecurity, to be identified by the Director of Consumer Protection
222 through rulemaking pursuant to subsection (a) of § 12D-106 of this chapter.

223 (2) The data broker is subject to the requirements of any federal or state law or regulation governing the
224 protection, security, or integrity of brokered personal information, and the data broker's information security program
225 conforms to the requirements of the applicable federal law or regulation.

226 (d) A violation of this section shall be deemed an unlawful practice under § 2513 of this title and a violation of
227 subchapter II of Chapter 25 of this title.

228 § 12D-105. Data Broker Fund

229 (a) There shall be a fund to be known as the Internet Privacy Protection Fund, which shall be credited by the State
230 Treasurer with all of the following:

231 (1) All fees received pursuant to § 12D-103 of this chapter.

232 (2) All funds received by the Department of Justice for any activity by the Consumer Protection Unit of the
233 Department of Justice to enforce the provisions of this chapter.

234 (b) Money in the Internet Privacy Protection Fund may be used for expenses incurred by the Consumer Protection
235 Unit of the Department of Justice in connection with any activity to carry out or enforce the provisions of this chapter,
236 including payment of salaries for personnel and costs, expenses incurred in administering the registration process set forth
237 in § 12D-103 of this chapter, charges incurred in the preparation, institution, and maintenance of investigations or
238 enforcement actions brought pursuant to the authority granted by this chapter, and consumer education and outreach
239 relating to information security and privacy.

240 § 12D-106. Regulations, Guidance, and Public Information.

241 (a) The Director of Consumer Protection shall promulgate regulations to carry out the purposes of this chapter,
242 which shall include identifying acceptable information security standards or frameworks for purposes of the safe harbor
243 provision of paragraph (c)(1) of § 12D-104 of this chapter, which may include:

244 (1) The National Institutes of Standards and Technology (NIST).

245 (2) The Federal Risk and Authorization Management Program.

246 (3) The Center for Internet Security.

247 (4) The Joint Technical Committee of the International Organization for Standardization and the International
248 Electrotechnical Commission.

249 (b) The Consumer Protection Unit of the Department of Justice shall make public on a searchable website the
250 information each data broker submits pursuant to paragraph (a)(3) of § 12D-103 of this chapter. The Consumer Protection
251 Unit of the Department of Justice shall update the website with the current year's registration information by April 30 of

252 each year. The Director of Consumer Protection may aggregate and analyze data broker registration information and make
253 the results of any such analysis public.

SYNOPSIS

This Act seeks to provide consumers with critical information about how their personal information is being used by data brokers. This Act requires data brokers to register with the Consumer Protection Unit of the Department of Justice and answer questions regarding their use of personal information that would be published online to inform consumers. A fee schedule is established based on the size of the data broker that would fund the enforcement of the statute. Entities or individuals who collect personal information but do not sell or license that personal data are not required to register. Registration only applies to data brokers who sell or license information. The Act prohibits acquiring or providing brokered personal information where it will be used for certain unlawful purposes, or where it was obtained through fraudulent means. The Act requires data brokers to protect brokered personal information.