

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

HOUSE BILL NO. 707

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the House Committee on Labor and Commerce

on \_\_\_\_\_)

(Patron Prior to Substitute--Delegate Maldonado)

A BILL to amend and reenact §§ 59.1-575, 59.1-578, and 59.1-580 of the Code of Virginia, relating to  
Consumer Data Protection Act; protections for children.

**Be it enacted by the General Assembly of Virginia:**

**1. That §§ 59.1-575, 59.1-578, and 59.1-580 of the Code of Virginia are amended and reenacted as follows:**

**§ 59.1-575. Definitions.**

As used in this chapter, unless the context requires a different meaning:

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-577, is the same consumer exercising such consumer rights with respect to the personal data at issue.

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

27 "Business associate" means the same meaning as the term established by HIPAA.

28 "Child" means any natural person younger than 13 years of age.

29 "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed,  
30 and unambiguous agreement to process personal data relating to the consumer. Consent may include a  
31 written statement, including a statement written by electronic means, or any other unambiguous  
32 affirmative action.

33 "Consumer" means a natural person who is a resident of the Commonwealth acting only in an  
34 individual or household context. It does not include a natural person acting in a commercial or employment  
35 context.

36 "Controller" means the natural or legal person that, alone or jointly with others, determines the  
37 purpose and means of processing personal data.

38 "Covered entity" means the same as the term is established by HIPAA.

39 "Decisions that produce legal or similarly significant effects concerning a consumer" means a  
40 decision made by the controller that results in the provision or denial by the controller of financial and  
41 lending services, housing, insurance, education enrollment, criminal justice, employment opportunities,  
42 health care services, or access to basic necessities, such as food and water.

43 "De-identified data" means data that cannot reasonably be linked to an identified or identifiable  
44 natural person, or a device linked to such person. A controller that possesses "de-identified data" shall  
45 comply with the requirements of subsection A of § 59.1-581.

46 "Health record" means the same as that term is defined in § 32.1-127.1:03.

47 "Health care provider" means the same as that term is defined in § 32.1-276.3.

48 "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42  
49 U.S.C. § 1320d et seq.).

50 "Identified or identifiable natural person" means a person who can be readily identified, directly  
51 or indirectly.

52 "Institution of higher education" means a public institution and private institution of higher  
53 education, as those terms are defined in § 23.1-100.

54 "Nonprofit organization" means any corporation organized under the Virginia Nonstock  
55 Corporation Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3),  
56 501(c)(6), or 501(c)(12) of the Internal Revenue Code, any political organization, any organization exempt  
57 from taxation under § 501(c)(4) of the Internal Revenue Code that is identified in § 52-41, and any  
58 subsidiary or affiliate of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

59 "Online service, product, or feature" means any service, product, or feature that is provided online.  
60 "Online service, product, or feature" does not include telecommunications service, as defined in 47 U.S.C.  
61 § 153, broadband Internet access service, as defined in 47 C.F.R. § 54.400, or delivery or use of a physical  
62 product.

63 "Personal data" means any information that is linked or reasonably linkable to an identified or  
64 identifiable natural person. "Personal data" does not include de-identified data or publicly available  
65 information.

66 "Political organization" means a party, committee, association, fund, or other organization,  
67 whether or not incorporated, organized and operated primarily for the purpose of influencing or attempting  
68 to influence the selection, nomination, election, or appointment of any individual to any federal, state, or  
69 local public office or office in a political organization or the election of a presidential/vice-presidential  
70 elector, whether or not such individual or elector is selected, nominated, elected, or appointed.

71 "Precise geolocation data" means information derived from technology, including but not limited  
72 to global positioning system level latitude and longitude coordinates or other mechanisms, that directly  
73 identifies the specific location of a natural person with precision and accuracy within a radius of 1,750  
74 feet. "Precise geolocation data" does not include the content of communications or any data generated by  
75 or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

76 "Process" or "processing" means any operation or set of operations performed, whether by manual  
77 or automated means, on personal data or on sets of personal data, such as the collection, use, storage,  
78 disclosure, analysis, deletion, or modification of personal data.

79 "Processor" means a natural or legal entity that processes personal data on behalf of a controller.

80 "Profiling" means any form of automated processing performed on personal data to evaluate,  
81 analyze, or predict personal aspects related to an identified or identifiable natural person's economic  
82 situation, health, personal preferences, interests, reliability, behavior, location, or movements.

83 "Protected health information" means the same as the term is established by HIPAA.

84 "Pseudonymous data" means personal data that cannot be attributed to a specific natural person  
85 without the use of additional information, provided that such additional information is kept separately and  
86 is subject to appropriate technical and organizational measures to ensure that the personal data is not  
87 attributed to an identified or identifiable natural person.

88 "Publicly available information" means information that is lawfully made available through  
89 federal, state, or local government records, or information that a business has a reasonable basis to believe  
90 is lawfully made available to the general public through widely distributed media, by the consumer, or by  
91 a person to whom the consumer has disclosed the information, unless the consumer has restricted the  
92 information to a specific audience.

93 "Sale of personal data" means the exchange of personal data for monetary consideration by the  
94 controller to a third party. "Sale of personal data" does not include:

- 95 1. The disclosure of personal data to a processor that processes the personal data on behalf of the  
96 controller;
- 97 2. The disclosure of personal data to a third party for purposes of providing a product or service  
98 requested by the consumer;
- 99 3. The disclosure or transfer of personal data to an affiliate of the controller;
- 100 4. The disclosure of information that the consumer (i) intentionally made available to the general  
101 public via a channel of mass media and (ii) did not restrict to a specific audience; or
- 102 5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger,  
103 acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the  
104 controller's assets.

105 "Sensitive data" means a category of personal data that includes:

- 106 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health
- 107 diagnosis, sexual orientation, or citizenship or immigration status;
- 108 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural
- 109 person;
- 110 3. The personal data collected from a known child; or
- 111 4. Precise geolocation data.

112 "State agency" means the same as that term is defined in § 2.2-307.

113 "Targeted advertising" means displaying advertisements to a consumer where the advertisement  
114 is selected based on personal data obtained from that consumer's activities over time and across  
115 nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted  
116 advertising" does not include:

- 117 1. Advertisements based on activities within a controller's own websites or online applications;
- 118 2. Advertisements based on the context of a consumer's current search query, visit to a website, or
- 119 online application;
- 120 3. Advertisements directed to a consumer in response to the consumer's request for information or
- 121 feedback; or
- 122 4. Processing personal data processed solely for measuring or reporting advertising performance,
- 123 reach, or frequency.

124 "Third party" means a natural or legal person, public authority, agency, or body other than the  
125 consumer, controller, processor, or an affiliate of the processor or the controller.

126 **§ 59.1-578. Data controller responsibilities; transparency.**

127 A. A controller shall:

- 128 1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in
- 129 relation to the purposes for which such data is processed, as disclosed to the consumer;
- 130 2. Except as otherwise provided in this chapter, not process personal data for purposes that are
- 131 neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data
- 132 is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

133 3. Establish, implement, and maintain reasonable administrative, technical, and physical data  
134 security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data  
135 security practices shall be appropriate to the volume and nature of the personal data at issue;

136 4. Not process personal data in violation of state and federal laws that prohibit unlawful  
137 discrimination against consumers. A controller shall not discriminate against a consumer for exercising  
138 any of the consumer rights contained in this chapter, including denying goods or services, charging  
139 different prices or rates for goods or services, or providing a different level of quality of goods and services  
140 to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide  
141 a product or service that requires the personal data of a consumer that the controller does not collect or  
142 maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods  
143 or services to a consumer, including offering goods or services for no fee, if the consumer has exercised  
144 his right to opt out pursuant to § 59.1-577 or the offer is related to a consumer's voluntary participation in  
145 a bona fide loyalty, rewards, premium features, discounts, or club card program;

146 5. Not process sensitive data concerning a consumer without obtaining the consumer's consent, or,  
147 in the case of the processing of sensitive data concerning a known child, without processing such data in  
148 accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

149 B. Any provision of a contract or agreement of any kind that purports to waive or limit in any way  
150 consumer rights pursuant to § 59.1-577 shall be deemed contrary to public policy and shall be void and  
151 unenforceable.

152 C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy  
153 notice that includes:

- 154 1. The categories of personal data processed by the controller;
- 155 2. The purpose for processing personal data;
- 156 3. How consumers may exercise their consumer rights pursuant § 59.1-577, including how a  
157 consumer may appeal a controller's decision with regard to the consumer's request;
- 158 4. The categories of personal data that the controller shares with third parties, if any; and
- 159 5. The categories of third parties, if any, with whom the controller shares personal data.

160 D. If a controller sells personal data to third parties or processes personal data for targeted  
161 advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner  
162 in which a consumer may exercise the right to opt out of such processing.

163 E. A controller shall establish, and shall describe in a privacy notice, one or more secure and  
164 reliable means for consumers to submit a request to exercise their consumer rights under this chapter.  
165 Such means shall take into account the ways in which consumers normally interact with the controller,  
166 the need for secure and reliable communication of such requests, and the ability of the controller to  
167 authenticate the identity of the consumer making the request. Controllers shall not require a consumer to  
168 create a new account in order to exercise consumer rights pursuant to § 59.1-577 but may require a  
169 consumer to use an existing account.

170 F. 1. Subject to the consent requirement established by subdivision 3, no controller shall process  
171 any personal data collected from a known child:

172 a. For the purposes of (i) targeted advertising, (ii) the sale of such personal data, or (iii) profiling  
173 in furtherance of decisions that produce legal or similarly significant effects concerning a consumer;

174 b. Unless such processing is reasonably necessary to provide the online service, product, or feature;

175 c. For any processing purpose other than the processing purpose that the controller disclosed at the  
176 time such controller collected such personal data or that is reasonably necessary for and compatible with  
177 such disclosed purpose; or

178 d. For longer than is reasonably necessary to provide the online service, product, or feature.

179 2. Subject to the consent requirement established by subdivision 3, no controller shall collect  
180 precise geolocation data from a known child unless (i) such precise geolocation data is reasonably  
181 necessary for the controller to provide an online service, product, or feature and, if such data is necessary  
182 to provide such online service, product, or feature, such controller shall only collect such data for the time  
183 necessary to provide such online service, product, or feature and (ii) the controller provides to the known  
184 child a signal indicating that such controller is collecting such precise geolocation data, which signal shall  
185 be available to such known child for the entire duration of such collection.

186 3. No controller shall engage in the activities described in subdivisions 1 or 2 unless the controller  
187 obtains consent from the child's parent or legal guardian in accordance with the federal Children's Online  
188 Privacy Protection Act (15 U.S.C. § 6501 et seq.).

189 **§ 59.1-580. Data protection assessments.**

190 A. A controller shall conduct and document a data protection assessment of each of the following  
191 processing activities involving personal data:

192 1. The processing of personal data for purposes of targeted advertising;

193 2. The sale of personal data;

194 3. The processing of personal data for purposes of profiling, where such profiling presents a  
195 reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on,  
196 consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion  
197 upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would  
198 be offensive to a reasonable person; or (iv) other substantial injury to consumers;

199 4. The processing of sensitive data; and

200 5. Any processing activities involving personal data that present a heightened risk of harm to  
201 consumers.

202 B. Each controller that offers any online service, product, or feature directed to consumers whom  
203 such controller has actual knowledge are children shall conduct a data protection assessment for such  
204 online service, product, or feature that addresses (i) the purpose of such online service, product, or feature;  
205 (ii) the categories of known children's personal data that such online service, product, or feature processes;  
206 and (iii) the purposes for which such controller processes known children's personal data with respect to  
207 such online service, product, or feature.

208 C. Data protection assessments conducted pursuant to ~~subsection A~~ this section shall identify and  
209 weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the  
210 consumer, other stakeholders, and the public against the potential risks to the rights of the consumer  
211 associated with such processing, as mitigated by safeguards that can be employed by the controller to  
212 reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as



213 the context of the processing and the relationship between the controller and the consumer whose personal  
214 data will be processed, shall be factored into this assessment by the controller.

215 ~~C-D.~~ The Attorney General may request, pursuant to a civil investigative demand, that a controller  
216 disclose any data protection assessment that is relevant to an investigation conducted by the Attorney  
217 General, and the controller shall make the data protection assessment available to the Attorney General.  
218 The Attorney General may evaluate the data protection assessment for compliance with the responsibilities  
219 set forth in § 59.1-578. Data protection assessments shall be confidential and exempt from public  
220 inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure  
221 of a data protection assessment pursuant to a request from the Attorney General shall not constitute a  
222 waiver of attorney-client privilege or work product protection with respect to the assessment and any  
223 information contained in the assessment.

224 ~~D-E.~~ A single data protection assessment may address a comparable set of processing operations  
225 that include similar activities.

226 ~~E-F.~~ Data protection assessments conducted by a controller for the purpose of compliance with  
227 other laws or regulations may comply under this section if the assessments have a reasonably comparable  
228 scope and effect.

229 ~~F-G.~~ Data protection assessment requirements shall apply to processing activities created or  
230 generated after January 1, 2023, and are not retroactive.

231 **2. That the provisions of this act shall become effective on January 1, 2025.**

232 #