

25103105D

SENATE BILL NO. 783

Offered January 8, 2025

Prefiled December 27, 2024

A BILL to amend and reenact §§ 59.1-575 and 59.1-576 of the Code of Virginia and to amend the Code of Virginia by adding a section numbered 59.1-577.1, relating to Consumer Data Protection Act; protections for children.

Patrons—Suetterlein and Mulchi

Referred to Committee on General Laws and Technology

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-575 and 59.1-576 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding a section numbered 59.1-577.1 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 are 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.

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

"Child" means any natural person younger than 18 years of age.

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

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

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

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

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

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

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

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

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

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

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

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

59 organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

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

64 "*Parent or guardian*" means the same as that term is defined in § 59.1-519.

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

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

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

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

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

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

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

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

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

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

96 1. The disclosure of personal data to a processor that processes the personal data on behalf of the
97 controller;

98 2. The disclosure of personal data to a third party for purposes of providing a product or service requested
99 by the consumer;

100 3. The disclosure or transfer of personal data to an affiliate of the controller;

101 4. The disclosure of information that the consumer (i) intentionally made available to the general public
102 via a channel of mass media and (ii) did not restrict to a specific audience; or

103 5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger,
104 acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the
105 controller's assets.

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

107 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis,
108 sexual orientation, or citizenship or immigration status;

109 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural 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 is
114 selected based on personal data obtained from that consumer's activities over time and across nonaffiliated
115 websites or online applications to predict such consumer's preferences or interests. "Targeted advertising"
116 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 online
119 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, reach, or
123 frequency.

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

126 "*Verifiable parental consent*" means authorization by a parent or guardian for a controller or processor
127 to register the child of such parent or guardian with such controller's or processor's product or service.

128 **§ 59.1-576. Scope; exemptions.**

129 A. This chapter applies to persons that conduct business in the Commonwealth or produce products or
130 services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or
131 process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000
132 consumers and derive over 50 percent of gross revenue from the sale of personal data.

133 B. This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or agency of
134 the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data
135 subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); (iii) covered entity or
136 business associate governed by the privacy, security, and breach notification rules issued by the U.S.
137 Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and
138 the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit
139 organization; or (v) institution of higher education.

140 C. The following information and data is exempt from this chapter:

141 1. Protected health information under HIPAA;

142 2. Health records for purposes of Title 32.1;

143 3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

144 4. Identifiable private information for purposes of the federal policy for the protection of human subjects
145 under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of
146 human subjects research pursuant to the good clinical practice guidelines issued by The International Council
147 for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human
148 subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research conducted in
149 accordance with the requirements set forth in this chapter, or other research conducted in accordance with
150 applicable law;

151 5. Information and documents created for purposes of the federal Health Care Quality Improvement Act
152 of 1986 (42 U.S.C. § 11101 et seq.);

153 6. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42
154 U.S.C. § 299b-21 et seq.);

155 7. Information derived from any of the health care-related information listed in this subsection that is de-
156 identified in accordance with the requirements for de-identification pursuant to HIPAA;

157 8. Information originating from, and intermingled to be indistinguishable with, or information treated in
158 the same manner as information exempt under this subsection that is maintained by a covered entity or
159 business associate as defined by HIPAA or a program or a qualified service organization as defined by 42
160 U.S.C. § 290dd-2;

161 9. Information used only for public health activities and purposes as authorized by HIPAA;

162 10. The collection, maintenance, disclosure, sale, communication, or use of any personal information
163 bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation,
164 personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides
165 information for use in a consumer report, and by a user of a consumer report, but only to the extent that such
166 activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

167 11. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy
168 Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

169 12. Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g
170 et seq.);

171 13. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act
172 (12 U.S.C. § 2001 et seq.); and

173 14. Data processed or maintained (i) in the course of an individual applying to, employed by, or acting as
174 an agent or independent contractor of a controller, processor, or third party, to the extent that the data is
175 collected and used within the context of that role; (ii) as the emergency contact information of an individual
176 under this chapter used for emergency contact purposes; or (iii) that is necessary to retain to administer
177 benefits for another individual relating to the individual under clause (i) and used for the purposes of
178 administering those benefits.

179 ~~D. Controllers and processors that comply with the verifiable parental consent requirements of the
180 Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any
181 obligation to obtain parental consent under this chapter.~~

182 **§ 59.1-577.1. Controller and processor responsibilities; verifiable parental consent.**

183 A. A controller or processor shall obtain verifiable parental consent prior to registering any child with
184 the controller's or processor's product or service or before collecting, using, or disclosing such child's
185 personal data that has been verified by such child's parent or guardian. A controller or processor shall give
186 the parent or guardian the option to consent to the collection and use of the child's personal data without
187 consenting to the disclosure of such child's personal data to third parties.

188 B. A controller or processor shall make reasonable efforts to obtain verifiable parental consent by taking
189 into consideration available technology to ensure that the person providing such consent is the child's parent
190 or guardian. Verifiable parental consent may be obtained from the parent or guardian by the parent or
191 guardian:

- 192 1. Providing a signed consent form to the controller or processor;
- 193 2. Using a credit card, debit card, or other online payment system that provides notification of any
194 transaction with the controller or processor to the primary account holder; or
- 195 3. Providing any valid government-issued identification to the controller or processor.