

24103305D

HOUSE BILL NO. 821

Offered January 10, 2024

Prefiled January 9, 2024

A BILL to amend and reenact §§ 59.1-575, 59.1-576, and 59.1-578 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.

Patron—Cherry

Referred to Committee on Labor and Commerce

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-575, 59.1-576, and 59.1-578 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 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 ~~13~~ 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

INTRODUCED

HB821

59 501(c)(12) of the Internal Revenue Code, any political organization, any organization exempt from
60 taxation under § 501(c)(4) of the Internal Revenue Code that is identified in § 52-41, and any subsidiary
61 or affiliate of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

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

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, whether or
67 not incorporated, organized and operated primarily for the purpose of influencing or attempting to
68 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 to
72 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
75 by 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 or
77 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, analyze,
81 or predict personal aspects related to an identified or identifiable natural person's economic situation,
82 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
86 and 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 federal,
89 state, or local government records, or information that a business has a reasonable basis to believe is
90 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 is
114 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.
116 "Targeted 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

feedback; or

4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

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

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

§ 59.1-576. Scope; exemptions.

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

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

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

1. Protected health information under HIPAA;

2. Health records for purposes of Title 32.1;

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

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

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

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

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

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

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

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

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

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

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

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

D. Controllers and processors that comply with the verifiable parental consent requirements of the

182 Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any
183 obligation to obtain parental consent under this chapter.

184 **§ 59.1-577.1. Controller and processor responsibilities; verifiable parental consent.**

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

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

194 1. Providing a signed consent form to the controller or processor;

195 2. Using a credit card, debit card, or other online payment system that provides notification of any
196 transaction with the controller or processor to the primary account holder; or

197 3. Providing any valid government-issued identification to the controller or processor.

198 **§ 59.1-578. Data controller responsibilities; transparency.**

199 A. A controller shall:

200 1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in
201 relation to the purposes for which such data is processed, as disclosed to the consumer;

202 2. Except as otherwise provided in this chapter, not process personal data for purposes that are
203 neither reasonably necessary nor compatible with the disclosed purposes for which such personal data
204 is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

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

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

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

222 6. Not knowingly process personal data of a child for purposes of (i) targeted advertising, (ii) the
223 sale of such personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly
224 significant effects concerning a consumer.

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

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

230 1. The categories of personal data processed by the controller;

231 2. The purpose for processing personal data;

232 3. How consumers may exercise their consumer rights pursuant § 59.1-577, including how a
233 consumer may appeal a controller's decision with regard to the consumer's request;

234 4. The categories of personal data that the controller shares with third parties, if any; and

235 5. The categories of third parties, if any, with whom the controller shares personal data.

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

239 E. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable
240 means for consumers to submit a request to exercise their consumer rights under this chapter. Such
241 means shall take into account the ways in which consumers normally interact with the controller, the
242 need for secure and reliable communication of such requests, and the ability of the controller to
243 authenticate the identity of the consumer making the request. Controllers shall not require a consumer to

- 244** create a new account in order to exercise consumer rights pursuant to § 59.1-577 but may require a
245 consumer to use an existing account.