24102711D

SENATE BILL NO. 361

Offered January 10, 2024

Prefiled January 9, 2024

A BILL to amend and reenact §§ 59.1-575 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.

Patrons—VanValkenburg and Suetterlein

Referred to Committee on Commerce and Labor

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-575 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" *or "minor"* 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.

"Covered user" means a user of a website, online service, or online or mobile application, or portion thereof, who is (i) actually known by the operator of a website, online service, or online or mobile application to be a minor or (ii) a user of a website, online service, or online or mobile application directed to minors.

"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.

"Directed to minors" means a website, online service, or online or mobile application, or a portion thereof, that is created for the purpose of reaching an audience that is predominantly composed of minors and that is not intended for a more general audience composed of adults. A website, online service, or online or mobile application, or portion thereof, is not directed to minors solely because such website, online service, or online or mobile application, or portion thereof, refers or links to any other website, online service, or online or mobile application directed to minors by using information

location tools, including a directory, index, reference, pointer, or hypertext link.

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

"Operator" means any person that operates or provides a website, online service, or online or mobile application and that:

1. Collects or maintains, either directly or through another person, personal data from or about the users of such website, online service, or online or mobile application;

2. Integrates with another website, online service, or online or mobile application and directly collects personal data from the users of such other website, online service, or online or mobile application;

3. Allows another person to collect personal data directly from users of such website, online service, or online or mobile application; or

4. Allows users of such website, online service, or online or mobile application to publicly disclose personal data.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

3. The personal data collected from a known child; or

4. Precise geolocation data.

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

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

1. Advertisements based on activities within a controller's own websites or online applications;

2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

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.

§ 59.1-577.1. Controller and processor responsibilities; children's privacy.

A. An operator shall not process, or allow a third party to process, the personal data of a covered user collected through the use of a website, online service, or online or mobile application unless:

1. The covered user is 12 years of age or younger and processing is permitted under 15 U.S.C. § 6502 and its implementing regulations; or

2. The covered user is 13 years of age or older and processing is strictly necessary or informed consent has been obtained.

For the purposes of this section, an operator shall treat a user as a covered user if the user's device communicates that the user is or should be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism. An operator shall adhere to any clear and unambiguous communications from a covered user's device, including through a browser plug-in or privacy setting, device setting, or other mechanism, concerning processing that the covered user consents to or declines to consent to.

B. For purposes of subdivision A 2, the processing of a covered user's personal data is permitted when it is strictly necessary for:

1. Providing or maintaining a specific product or service requested by the covered user;

2. Conducting the operator's internal business operations. Such internal business operations do not include any activities related to marketing, advertising, or providing products or services to third parties, or prompting covered users to use the website, online service, or online or mobile application when it is not in use;

3. Identifying and repairing technical errors that impair existing or intended functionality;

4. Protecting against malicious, fraudulent, or illegal activity;

5. Investigating, establishing, exercising, preparing for, or defending legal claims;

6. Complying with federal, state, or local laws, rules, or regulations;

7. Complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

8. Detecting, responding to, or preventing security incidents or threats; or

9. Protecting the vital interests of a natural person.

C. For purposes of subdivision A 2, to process personal data of a covered user where such processing is not strictly necessary under subsection B, informed consent must be obtained from the covered user either through a device communication or through a request. Requests for such informed consent shall:

1. Be made separately from any other transaction or part of a transaction;

2. Be made in the absence of any mechanism that has the purpose or substantial effect of obscuring, subverting, or impairing a covered user's decision-making regarding authorization for the processing;

3. Allow the covered user to provide or withhold consent separately for each type of processing, if requesting informed consent for multiple types of processing;

4. State, clearly and conspicuously, that the processing is optional and that the covered user may decline without preventing continued use of the website, online service, or online or mobile application; and

5. Present a clear option to refuse to provide consent.

D. Informed consent, once given, shall be revocable at any time by a covered user and shall be as easy to revoke as it was to provide. No requests for informed consent for processing shall be made by an operator for one calendar year if (i) a covered user revokes or declines to provide such informed consent or (ii) a covered user's device communicates that the covered user declines to provide such informed consent.

E. No operator shall withhold, degrade, lower the quality of, or increase the price of any product, service, or feature to a covered user due to the operator not obtaining verifiable parental consent under 15 U.S.C. § 6502 and its implementing regulations or informed consent under subsection C except where processing is strictly necessary to provide a product, service, or feature.

F. Within 14 days of determining that a user is a covered user, an operator shall:

1. Dispose of, destroy, or delete all personal data of such covered user that it maintains, unless processing such personal data is permitted under 15 U.S.C. § 6502 and its implementing regulations, is strictly necessary under subsection B, or informed consent is obtained as set forth in subsection C; and

2. Notify any third parties to whom it disclosed the personal data and any third parties it allowed to process the personal data that the user is a covered user.

G. No operator shall disclose the personal data of a covered user to a third party, or allow the processing of the personal data of a covered user by a third party, without a written, binding agreement governing such disclosure or processing. Such agreement shall clearly set forth instructions for the nature and purpose of the third party's processing of the personal data, instructions for using or further disclosing the personal data, and the rights and obligations of both parties. Prior to disclosing personal data to a third party, the operator shall inform the third party if such data is the personal data of a covered user. An agreement pursuant to this subsection shall require that the third party:

1. Process the personal data of covered users only to the extent strictly necessary or where informed consent was obtained;

2. Delete or return to the operator all personal data of covered users at the end of its provision of services, unless retention of the personal data is required by law;

3. Make available, upon reasonable request of the operator, all data in its possession necessary to demonstrate the third party's compliance with the obligations in this section;

4. Allow, and cooperate with, reasonable assessments by the operator for purposes of evaluating compliance with the obligations of this section; and

5. Notify the operator a reasonable time in advance before disclosing or transferring the personal data of covered users to any additional third parties, which may be in the form of a regularly updated list of additional third parties that may access personal data of covered users.

H. No operator shall process the personal data of any user in a manner not previously permitted unless and until it receives informed consent upon learning that such user is no longer a covered user.

I. Nothing in this section shall be construed to apply to an operator processing the personal data of a covered user of another website, online service, or online or mobile application, or portion thereof, where such operator received reasonable written representations that the covered user provided informed consent for such processing or the operator does not have actual knowledge that (i) the covered user is a minor and (ii) the other website, online service, or online or mobile application, or portion thereof, is directed to minors.

J. Any violation of this section may be prosecuted in accordance with the procedures established in § 59.1-584.

§ 59.1-578. Data controller responsibilities; transparency.

A. A controller shall:

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

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

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

4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging

different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-577 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; ~~and~~

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

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

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

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

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

2. The purpose for processing personal data;

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

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

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

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

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