25102628D

HOUSE BILL NO. 2043

Offered January 8, 2025

Prefiled January 7, 2025

A BILL to amend and reenact §§ 59.1-575*,* 59.1-578*, and* 59.1-584 *of the Code of Virginia and to amend the Code of Virginia by adding sections numbered* 59.1-579.1 *and* 59.1-579.2*, relating to Consumer Data Protection Act; user-generated content protected; civil penalty.*

Patron—Anthony

Committee Referral Pending

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-575, 59.1-578, and 59.1-584 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding sections numbered 59.1-579.1 and 59.1-579.2 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 13 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 §

INTRODUCED

HB2043

1/7/25 09:54

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.

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

"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.

"Secondary use" means the processing of personal data or user-generated content for purposes other than those disclosed at the time of consent by the consumer.

"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.

"User-generated content" means any digital content, including text, images, video, audio, or other content , that is produced by a consumer.

§ 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.).

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 *or user-generated content* processed by the controller;

2. The purpose for processing personal data *or user-generated content*;

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 *or user-generated content* 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 *or user-generated content; and*

6. The secondary uses, if any, of the consumer's personal data or user-generated content and corresponding mechanisms for how a consumer may consent to such uses.

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.

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

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

c. For any processing purpose other than the processing purpose that the controller disclosed at the time

such controller collected such personal data or that is reasonably necessary for and compatible with such disclosed purpose; or

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

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

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

§ 59.1-579.1. Secondary use.

No controller or processor shall process the personal data or user-generated content of consumers for purposes other than those consented to by the consumer, unless such controller or processor obtains consent from the consumer for any secondary use of personal data or user-generated content.

§ 59.1-579.2. Reporting requirement.

Upon request by a consumer, a controller or processor shall provide a report to such consumer that describes, over the prior 12 months:

1. The categories of such consumer's personal data or user-generated content that were processed by the controller or processor;

2. The purposes for processing such consumer's personal data or user-generated content;

3. The categories of such consumer's personal data or user-generated content that the controller or processor shared with third parties, if any;

4. The categories of third parties, if any, with whom the controller or processor shared the consumer's personal data or user-generated content; and

5. The secondary uses, if any, of the consumer's personal data or user-generated content.

A controller or processor shall furnish such report to a consumer within 90 days after such consumer submits a request to such controller or processor pursuant to this section.

§ 59.1-584. Enforcement; civil penalty; expenses.

A. ~~The Attorney General shall have exclusive authority to enforce the provisions of this chapter.~~

~~B.~~ Prior to initiating any action under this chapter, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

~~C.~~ *B.* If a controller or processor continues to violate this chapter following the cure period in subsection ~~B~~ *A* or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to ~~$7,500~~ *$15,000* for each violation under this chapter*, or for repeated noncompliance with or egregious violations of this chapter, up to $22,500 per violation*. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Regulatory, Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund.

~~D.~~ *C.* The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

~~E. Nothing in this chapter shall be construed as providing the basis for, or be subject to,~~ *D. Any consumer who suffers a loss by reason of a violation of any provision of this chapter may bring* a private right of action ~~for violations of this chapter or under any other law~~ *against a controller or processor. Any consumer who is successful in such action shall recover reasonable attorney fees, expert witness fees, and court costs incurred by bringing such action.*