26100794D

SENATE BILL NO. 232

Offered January 14, 2026

A BILL to amend and reenact §§ 59.1-575, 59.1-576, and 59.1-577 of the Code of Virginia and to amend the Code of Virginia by adding sections numbered 59.1-577.2 and 59.1-577.3, relating to Consumer Data Protection Act; prohibitions and duties relating to minors.

Patron—Head

Referred to Committee on General Laws and Technology

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-575, 59.1-576, and 59.1-577 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding sections numbered 59.1-577.2 and 59.1-577.3 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, *a* 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.

"Child pornography" means the same as that term is defined in § 18.2-374.1.

"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~~ *"Consumer"* 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.

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

"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation Act

INTRODUCED

SB232

7/29/26 11:43

(§ 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.

"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.

"Parent" means a parent or legal guardian of a child or minor.

"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.

"Social media platform" means a public or semipublic Internet-based service or application that has users in the Commonwealth and that meets the following criteria:

1. Connects users in order to allow users to interact socially with each other within such service or application. No service or application that exclusively provides email or direct messaging services shall be considered to meet this criterion on the basis of that function alone; and

2. Allows users to do all of the following:

a. Construct a public or semipublic profile for purposes of signing into and using such service or application;

b. Populate a public list of other users with whom such user shares a social connection within such service or application; and

c. Create or post content viewable by other users, including content on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users. No service or application that consists primarily of news, sports, entertainment, ecommerce, or content preselected by the provider and not generated by users, and for which any chat, comments, or interactive functionality is incidental to, directly related to, or dependent on the provision of such content, or that is for interactive gaming, shall be considered to meet this criterion on the basis of that function alone.

"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" means a person not acting as an agent of a controller or processor.

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

§ 59.1-577. Personal data rights; consumers.

A. A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known ~~child's~~ *minor's* parent ~~or legal guardian~~ may invoke such consumer rights on behalf of the ~~child~~ *minor* regarding processing personal data belonging to the known ~~child~~ *minor*. A controller shall comply with an authenticated consumer request to exercise the right *to*:

1. ~~To confirm~~ *Confirm* whether or not a controller is processing the consumer's personal data and to access such personal data;

2. ~~To correct~~ *Correct* inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

3. ~~To delete~~ *Delete* personal data provided by or obtained about the consumer;

4. ~~To obtain~~ *Obtain* a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

5. ~~To opt~~ *Opt* out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

B. *A parent of a minor may invoke additional consumer rights on behalf of the minor pursuant to this subsection at any time by submitting a request to a controller of an online service, product, or feature specifying the consumer rights the parent wishes to invoke. Such controller shall comply with an authenticated consumer request to exercise the right of a parent to obtain a copy of all data in the controller's possession associated with the minor, organized by type of data and the purpose for which the controller processed each type of data. Such copy shall include, as applicable, (i) the name of each third party to which the controller disclosed such data; (ii) each source other than the minor from which the controller obtained such data; (iii) the length of time for which the controller will retain the data associated with the minor; (iv) any index or score assigned to the minor as a result of the data, including whether the controller created the index or score and, if not, who created the index or score; and (v) the manner in which the controller uses such index or score. Such controller may require a minor's parent to confirm such parent's identity using a method acceptable under subsection B of § 59.1-577.2.*

C. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized ~~pursuant to subsection A~~ *by this section* as follows:

1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in ~~subsection A~~ *this section*. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

2. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection ~~C~~ *D*.

3. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating

the manifestly unfounded, excessive, or repetitive nature of the request.

4. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under ~~subsection A~~ *this section* and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

5. A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision A 3 by either (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using such retained data for any other purpose pursuant to the provisions of this chapter or (ii) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of this chapter.

~~C.~~ *D.* A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision ~~B~~ *C* 2. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

§ 59.1-577.1. Social media platforms; responsibilities and prohibitions related to minors.

A. ~~For purposes of this section, "minor" means any natural person younger than 16 years of age.~~

~~B.~~ Any controller or processor that operates a social media platform shall (i) use commercially reasonable methods, such as a neutral age screen mechanism, to determine whether a user is a minor and (ii) limit a minor's use of such social media platform to one hour per day, per service or application, and allow a parent to give verifiable parental consent to increase or decrease the daily time limit. *Controllers and processors that obtain verified consent pursuant to subsection B of § 59.1-577.2 shall be deemed compliant with any obligation to obtain parental consent under this section.*

~~C.~~ *B.* Information collected for the purpose of determining a user's age shall not be used for any purpose other than age determination and provision of age-appropriate experiences. For purposes of this section, any controller or processor that operates a social media platform shall treat a user as a minor if the user's device communicates or signals that the user is or shall be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism.

~~D. Nothing in this section shall be construed as requiring any controller or processor that operates a social media platform to give a parent who grants verifiable parental consent pursuant to subsection B any additional or special access to or control over the data or accounts of the minor.~~

~~E.~~ *C.* No controller or processor that operates a social media platform shall withhold, degrade, lower the quality of, or increase the price of any online service, product, or feature to a user due to the controller or processor not being permitted to provide use of such social media platform beyond the one hour per day, per service or application, daily time limit under subsection ~~B~~ *A*. However, nothing in this section shall be construed as (i) requiring a social media platform to provide an online service, product, or feature that requires the personal information of a known minor or (ii) prohibiting a social media platform from offering a different price, rate, level, quality, or selection of goods or services to a known minor, including offering goods or services for no fee, if such behavior is reasonably related to the exercise of rights pursuant to or compliance with the requirements of this chapter.

§ 59.1-577.2. Prohibition on agreements with minors; exemption for parental consent.

A. Except as provided by this section, no controller of an online service, product, or feature shall enter into a terms of service agreement, a user agreement, or an agreement to create an account for an online service, product, or feature if such agreement is with a known minor.

B. A controller of an online service, product, or feature may enter into a terms of service agreement, a user agreement, or an agreement to create an account for an online service, product, or feature with a known minor if such minor's parent provides verified consent as provided by this subsection. Such controller may obtain verified consent by any of the following methods:

1. Providing a form for the minor's parent to sign and return to the controller by common carrier, facsimile, or electronic scan;

2. Providing a toll-free telephone number for the minor's parent to call to consent;

3. Coordinating a call with the minor's parent over videoconferencing technology;

4. Collecting information related to the minor's parent's government-issued identification and deleting such information after confirming the identity of the parent;

5. Allowing the minor's parent to provide consent by responding to an email and taking additional steps to verify the parent's identity; and

6. Any other commercially reasonable method of obtaining consent.

C. At the time of obtaining verified consent from a parent on behalf of a minor for entering into a terms of service agreement, a user agreement, or an agreement to create an account for an online service, product, or feature, a controller of an online service, product, or feature shall provide the parent with the ability to:

1. Enable the highest privacy setting offered by the controller;

2. Prevent the controller from collecting any data associated with the minor that is not necessary to provide the online service, product, or feature;

3. Prevent the controller from processing any data associated with the minor in a manner that is not related to the purpose for which the data was collected;

4. Prevent the controller from sharing, disclosing, or transferring data associated with the minor in exchange for monetary or other valuable consideration;

5. Prevent the collection of precise geolocation data by the controller;

6. Prevent the display of targeted advertising for the minor; or

7. Prevent the minor from making purchases or financial transactions.

§ 59.1-577.3. Duties owed to minors; online services, products, features.

A. A controller of an online service, product, or feature that allows advertisers to advertise to known minors on the online service, product, or feature shall disclose in a clear and accessible manner at the time the advertisement is displayed:

1. The name of the product, service, or brand;

2. The subject matter of each advertisement or marketing material;

3. If the controller or advertiser targets advertisements to known minors, the reason why the advertisement has been targeted to minors;

4. The way in which data associated with a known minor's use of the online service, product, or feature leads to the advertisement targeted to the minor; and

5. Whether certain media are advertisements.

B. A controller of an online service, product, or feature that uses algorithms to automate the suggestion, promotion, or ranking of information to known minors on the online service, product, or feature shall:

1. Ensure that the algorithm does not interfere with the controller's duties under subsection C; and

2. Disclose in the controller's terms of service, in a clear and accessible manner, an overview of the manner in which (i) the online service, product, or feature uses algorithms to provide information to known minors and (ii) those algorithms use data associated with the minor.

C. In relation to a known minor's use of an online service, product, or feature, a controller of an online service, product, or feature shall exercise reasonable care to prevent:

1. Self-harm, suicide, eating disorders, and other similar behaviors;

2. Substance abuse and patterns of use that indicate addiction;

3. Bullying and harassment;

4. Sexual exploitation, including enticement, grooming, trafficking, abuse, and child pornography;

5. Advertisements for products or services that are unlawful for a minor, including illegal drugs, tobacco, gambling, pornography, and alcohol; and

6. Predatory, unfair, or deceptive marketing practices.

2. That the provisions of this act shall become effective on January 1, 2027.