Chapter 53. Consumer Data Protection Act.

§ 59.1-575. (Effective until January 1, 2025) 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 years of age.

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

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

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

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

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

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

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

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

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

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

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

"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code, any political organization, any organization exempt from taxation under § 501(c)(4) of the Internal Revenue Code that is identified in § 52-41, and any subsidiary or affiliate of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

"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.

2021, Sp. Sess. I, cc. 35, 36; 2022, cc. 451, 452.

§ 59.1-575. (Effective January 1, 2025) 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 years of age.

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

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

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

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

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment,

criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

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

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

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

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

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

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

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

"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.

2021, Sp. Sess. I, cc. 35, 36; 2022, cc. 451, 452; 2024, cc. 840, 844.

§ 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.

2021, Sp. Sess. I, cc. 35, 36.

§ 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 parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the

known child. A controller shall comply with an authenticated consumer request to exercise the right:

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

2. To 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 personal data provided by or obtained about the consumer;

4. To 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 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. 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 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. 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.

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 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. 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 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.

2021, Sp. Sess. I, cc. 35, 36; 2022, c. 423.

§ 59.1-578. (Effective until January 1, 2025) 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 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.

2021, Sp. Sess. I, cc. 35, 36.

§ 59.1-578. (Effective January 1, 2025) 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 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.

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.).

2021, Sp. Sess. I, cc. 35, 36; 2024, cc. 840, 844.

§ 59.1-579. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-577.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-580.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

2021, Sp. Sess. I, cc. 35, 36.

§ 59.1-580. (Effective until January 1, 2025) Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;

2. The sale of personal data;

3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

4. The processing of sensitive data; and

5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

C. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-578. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

D. A single data protection assessment may address a comparable set of processing operations that include similar activities.

E. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

F. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

2021, Sp. Sess. I, cc. 35, 36.

§ 59.1-580. (Effective January 1, 2025) Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;

2. The sale of personal data;

3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

4. The processing of sensitive data; and

5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Each controller that offers any online service, product, or feature directed to consumers whom such controller has actual knowledge are children shall conduct a data protection assessment for such online service, product, or feature that addresses (i) the purpose of such online service, product, or feature; (ii) the categories of known children's personal data that such online service, product, or feature processes; and (iii) the purposes for which such controller processes known children's personal data with respect to such online service, product, or feature.

C. Data protection assessments conducted pursuant to this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing

and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

D. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-578. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

E. A single data protection assessment may address a comparable set of processing operations that include similar activities.

F. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

G. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

2021, Sp. Sess. I, cc. 35, 36; 2024, cc. 840, 844.

§ 59.1-581. Processing de-identified data; exemptions.

A. The controller in possession of de-identified data shall:

1. Take reasonable measures to ensure that the data cannot be associated with a natural person;

2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

B. Nothing in this chapter shall be construed to (i) require a controller or processor to re-identify de-identified data or pseudonymous data or (ii) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

C. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to § 59.1-577, if all of the following are true:

1. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

2. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

D. The consumer rights contained in subdivisions A 1 through 4 of § 59.1-577 and § 59.1-578 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

2021, Sp. Sess. I, cc. 35, 36.

§ 59.1-582. Limitations.

A. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

1. Comply with federal, state, or local laws, rules, or regulations;

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

3. Cooperate with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

4. Investigate, establish, exercise, prepare for, or defend legal claims;

5. Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

6. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

8. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine: (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

9. Assist another controller, processor, or third party with any of the obligations under this subsection.

B. The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to:

1. Conduct internal research to develop, improve, or repair products, services, or technology;

2. Effectuate a product recall;

3. Identify and repair technical errors that impair existing or intended functionality; or

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

C. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an

evidentiary privilege under the laws of the Commonwealth. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the Commonwealth as part of a privileged communication.

D. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives such personal data.

E. Nothing in this chapter shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

F. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

1. Reasonably necessary and proportionate to the purposes listed in this section; and

2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection B shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

G. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection F.

H. Processing personal data for the purposes expressly identified in subdivisions A 1 through 9 shall not solely make an entity a controller with respect to such processing.

2021, Sp. Sess. I, cc. 35, 36.

§ 59.1-583. Investigative authority.

Whenever the Attorney General has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the Attorney General is empowered to issue a civil investigative demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued under this section.

2021, Sp. Sess. I, cc. 35, 36.

§ 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. If a controller or processor continues to violate this chapter following the cure period in subsection B 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 for each violation under this chapter. 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. 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, a private right of action for violations of this chapter or under any other law.

2021, Sp. Sess. I, cc. 35, 36; 2022, cc. 451, 452.

§ 59.1-585. Repealed.

Repealed by Acts 2022, cc. 451 and 452, cl. 2.