20103007D

HOUSE BILL NO. 473

Offered January 8, 2020
Prefiled January 3, 2020

A BILL to amend and reenact § 59.1-200 of the Code of Virginia and to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-579, relating to the management and oversight of personal data.

Patron—Sickles

Committee Referral Pending

Be it enacted by the General Assembly of Virginia:

1. That § 59.1-200 of the Code of Virginia is amended and reenacted and that the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-579, as follows:

§ 59.1-200. Prohibited practices.

A. The following fraudulent acts or practices committed by a supplier in connection with a consumer transaction are hereby declared unlawful:

1. Misrepresenting goods or services as those of another;

2. Misrepresenting the source, sponsorship, approval, or certification of goods or services;

3. Misrepresenting the affiliation, connection, or association of the supplier, or of the goods or services, with another;

4. Misrepresenting geographic origin in connection with goods or services;

5. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

6. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model;

7. Advertising or offering for sale goods that are used, secondhand, repossessed, defective, blemished, deteriorated, or reconditioned, or that are "seconds," irregulars, imperfects, or "not first class," without clearly and unequivocally indicating in the advertisement or offer for sale that the goods are used, secondhand, repossessed, defective, blemished, deteriorated, reconditioned, or are "seconds," irregulars, imperfects or "not first class";

8. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell at the price or upon the terms advertised.

In any action brought under this subdivision, the refusal by any person, or any employee, agent, or servant thereof, to sell any goods or services advertised or offered for sale at the price or upon the terms advertised or offered, shall be prima facie evidence of a violation of this subdivision. This paragraph shall not apply when it is clearly and conspicuously stated in the advertisement or offer by which such goods or services are advertised or offered for sale, that the supplier or offeror has a limited quantity or amount of such goods or services for sale, and the supplier or offeror at the time of such advertisement or offer did in fact have or reasonably expected to have at least such quantity or amount for sale;

9. Making false or misleading statements of fact concerning the reasons for, existence of, or amounts of price reductions;

10. Misrepresenting that repairs, alterations, modifications, or services have been performed or parts installed;

11. Misrepresenting by the use of any written or documentary material that appears to be an invoice or bill for merchandise or services previously ordered;

12. Notwithstanding any other provision of law, using in any manner the words "wholesale," "wholesaler," "factory," or "manufacturer" in the supplier's name, or to describe the nature of the supplier's business, unless the supplier is actually engaged primarily in selling at wholesale or in manufacturing the goods or services advertised or offered for sale;

13. Using in any contract or lease any liquidated damage clause, penalty clause, or waiver of defense, or attempting to collect any liquidated damages or penalties under any clause, waiver, damages, or penalties that are void or unenforceable under any otherwise applicable laws of the Commonwealth, or under federal statutes or regulations;

13a. Failing to provide to a consumer, or failing to use or include in any written document or material provided to or executed by a consumer, in connection with a consumer transaction any statement, disclosure, notice, or other information however characterized when the supplier is required by 16 C.F.R. Part 433 to so provide, use, or include the statement, disclosure, notice, or other information in connection with the consumer transaction;

14. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction;

15. Violating any provision of § 3.2-6512, 3.2-6513, or 3.2-6516, relating to the sale of certain animals by pet dealers which is described in such sections, is a violation of this chapter;

16. Failing to disclose all conditions, charges, or fees relating to:

a. The return of goods for refund, exchange, or credit. Such disclosure shall be by means of a sign attached to the goods, or placed in a conspicuous public area of the premises of the supplier, so as to be readily noticeable and readable by the person obtaining the goods from the supplier. If the supplier does not permit a refund, exchange, or credit for return, he shall so state on a similar sign. The provisions of this subdivision shall not apply to any retail merchant who has a policy of providing, for a period of not less than 20 days after date of purchase, a cash refund or credit to the purchaser's credit card account for the return of defective, unused, or undamaged merchandise upon presentation of proof of purchase. In the case of merchandise paid for by check, the purchase shall be treated as a cash purchase and any refund may be delayed for a period of 10 banking days to allow for the check to clear. This subdivision does not apply to sale merchandise that is obviously distressed, out of date, post season, or otherwise reduced for clearance; nor does this subdivision apply to special order purchases where the purchaser has requested the supplier to order merchandise of a specific or unusual size, color, or brand not ordinarily carried in the store or the store's catalog; nor shall this subdivision apply in connection with a transaction for the sale or lease of motor vehicles, farm tractors, or motorcycles as defined in § 46.2-100;

b. A layaway agreement. Such disclosure shall be furnished to the consumer (i) in writing at the time of the layaway agreement, or (ii) by means of a sign placed in a conspicuous public area of the premises of the supplier, so as to be readily noticeable and readable by the consumer, or (iii) on the bill of sale. Disclosure shall include the conditions, charges, or fees in the event that a consumer breaches the agreement;

16a. Failing to provide written notice to a consumer of an existing open-end credit balance in excess of $5 (i) on an account maintained by the supplier and (ii) resulting from such consumer's overpayment on such account. Suppliers shall give consumers written notice of such credit balances within 60 days of receiving overpayments. If the credit balance information is incorporated into statements of account furnished consumers by suppliers within such 60-day period, no separate or additional notice is required;

17. If a supplier enters into a written agreement with a consumer to resolve a dispute that arises in connection with a consumer transaction, failing to adhere to the terms and conditions of such an agreement;

18. Violating any provision of the Virginia Health Club Act, Chapter 24 (§ 59.1-294 et seq.);

19. Violating any provision of the Virginia Home Solicitation Sales Act, Chapter 2.1 (§ 59.1-21.1 et seq.);

20. Violating any provision of the Automobile Repair Facilities Act, Chapter 17.1 (§ 59.1-207.1 et seq.);

21. Violating any provision of the Virginia Lease-Purchase Agreement Act, Chapter 17.4 (§ 59.1-207.17 et seq.);

22. Violating any provision of the Prizes and Gifts Act, Chapter 31 (§ 59.1-415 et seq.);

23. Violating any provision of the Virginia Public Telephone Information Act, Chapter 32 (§ 59.1-424 et seq.);

24. Violating any provision of § 54.1-1505;

25. Violating any provision of the Motor Vehicle Manufacturers' Warranty Adjustment Act, Chapter 17.6 (§ 59.1-207.34 et seq.);

26. Violating any provision of § 3.2-5627, relating to the pricing of merchandise;

27. Violating any provision of the Pay-Per-Call Services Act, Chapter 33 (§ 59.1-429 et seq.);

28. Violating any provision of the Extended Service Contract Act, Chapter 34 (§ 59.1-435 et seq.);

29. Violating any provision of the Virginia Membership Camping Act, Chapter 25 (§ 59.1-311 et seq.);

30. Violating any provision of the Comparison Price Advertising Act, Chapter 17.7 (§ 59.1-207.40 et seq.);

31. Violating any provision of the Virginia Travel Club Act, Chapter 36 (§ 59.1-445 et seq.);

32. Violating any provision of §§ 46.2-1231 and 46.2-1233.1;

33. Violating any provision of Chapter 40 (§ 54.1-4000 et seq.) of Title 54.1;

34. Violating any provision of Chapter 10.1 (§ 58.1-1031 et seq.) of Title 58.1;

35. Using the consumer's social security number as the consumer's account number with the supplier, if the consumer has requested in writing that the supplier use an alternate number not associated with the consumer's social security number;

36. Violating any provision of Chapter 18 (§ 6.2-1800 et seq.) of Title 6.2;

37. Violating any provision of § 8.01-40.2;

38. Violating any provision of Article 7 (§ 32.1-212 et seq.) of Chapter 6 of Title 32.1;
39. Violating any provision of Chapter 34.1 (§ 59.1-441.1 et seq.);
40. Violating any provision of Chapter 20 (§ 6.2-2000 et seq.) of Title 6.2;
41. Violating any provision of the Virginia Post-Disaster Anti-Price Gouging Act, Chapter 46 (§ 59.1-525 et seq.);
42. Violating any provision of Chapter 47 (§ 59.1-530 et seq.);
43. Violating any provision of § 59.1-443.2;
44. Violating any provision of Chapter 48 (§ 59.1-533 et seq.);
45. Violating any provision of Chapter 25 (§ 6.2-2500 et seq.) of Title 6.2;
46. Violating the provisions of clause (i) of subsection B of § 54.1-1115;
47. Violating any provision of § 18.2-239;
48. Violating any provision of Chapter 26 (§ 59.1-336 et seq.);
49. Selling, offering for sale, or manufacturing for sale a children's product the supplier knows or has reason to know was recalled by the U.S. Consumer Product Safety Commission. There is a rebuttable presumption that a supplier has reason to know a children's product was recalled if notice of the recall has been posted continuously at least 30 days before the sale, offer for sale, or manufacturing for sale on the website of the U.S. Consumer Product Safety Commission. This prohibition does not apply to children's products that are used, secondhand or "seconds";
50. Violating any provision of Chapter 44.1 (§ 59.1-518.1 et seq.);
51. Violating any provision of Chapter 22 (§ 6.2-2200 et seq.) of Title 6.2;
52. Violating any provision of § 8.2-317.1;
53. Violating subsection A of § 9.1-149.1;
54. Selling, offering for sale, or using in the construction, remodeling, or repair of any residential dwelling in the Commonwealth, any drywall that the supplier knows or has reason to know is defective drywall. This subdivision shall not apply to the sale or offering for sale of any building or structure in which defective drywall has been permanently installed or affixed;
55. Engaging in fraudulent or improper or dishonest conduct as defined in § 54.1-1118 while engaged in a transaction that was initiated (i) during a declared state of emergency as defined in § 44-146.16 or (ii) to repair damage resulting from the event that prompted the declaration of a state of emergency, regardless of whether the supplier is licensed as a contractor in the Commonwealth pursuant to Chapter 11 (§ 54.1-1100 et seq.) of Title 54.1;
56. Violating any provision of Chapter 33.1 (§ 59.1-434.1 et seq.);
57. Violating any provision of § 18.2-178, 18.2-178.1, or 18.2-200.1;
58. Violating any provision of Chapter 17.8 (§ 59.1-207.45 et seq.);
59. Violating any provision of subsection E of § 32.1-126; ~~and~~
60. Violating any provision of § 54.1-111 relating to the unlicensed practice of a profession licensed under Chapter 11 (§ 54.1-1100 et seq.) or Chapter 21 (§ 54.1-2100 et seq.) of Title 54.1*; and*
61. Violating any provision of Chapter 52 (§ 59.1-571 et seq.).

B. Nothing in this section shall be construed to invalidate or make unenforceable any contract or lease solely by reason of the failure of such contract or lease to comply with any other law of the Commonwealth or any federal statute or regulation, to the extent such other law, statute, or regulation provides that a violation of such law, statute, or regulation shall not invalidate or make unenforceable such contract or lease.

CHAPTER 52.
VIRGINIA PRIVACY ACT.

§ 59.1-571. 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.

"Business associate" has the meaning ascribed thereto in 45 C.F.R. § 160.103.

"Business purpose" means the processing of personal data for the controller's or its processor's operational purposes, or other notified purposes, provided that the processing of personal data shall be reasonably necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed or for another operational purpose that is compatible with the context in which the personal data was collected. "Business purpose" includes:

1. Auditing related to a current interaction with the consumer and concurrent transactions, including counting advertising impressions, verifying positioning and quality of advertising impressions, and auditing compliance with this specification and other standards;

2. Detecting security incidents; protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for such activity;

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

4. Short-term, transient use, provided that the personal data is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including the contextual customization of advertiements shown as part of the same interaction;

5. Maintaining or servicing accounts, providing consumer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;

6. Undertaking internal research for technological development; or

7. Authenticating a consumer's identity.

"Child" means any natural person under 13 years of age.

"Consent" means a clear affirmative act signifying a specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

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

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

"Covered entity" has the meaning ascribed thereto in 45 C.F.R. § 160.103.

"Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker. As used in this definition, "sells or licenses" does not include (i) a one-time or occasional sale of assets that is not part of the ordinary conduct of the business; (ii) a sale or license of data that is merely incidental to the business; or (iii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier.

"Deidentified data" means:

1. Data that cannot be linked to a known natural person without additional information kept separately; or

2. Data (i) that has been modified to a degree that the risk of reidentification is small, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, and (iii) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls.

"Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

"Health care facility" means any institution, place, building, or agency required to be licensed under Virginia law, including but not limited to any hospital, nursing facility or nursing home, boarding home, assisted living facility, supervised living facility, or ambulatory medical and surgical center.

"Health care information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of chemical base pairs. "Health care information" includes any required accounting of disclosures of health care information.

"Health care provider" means any physician, hospital, or other person that is licensed or otherwise authorized in the Commonwealth to furnish health care services.

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

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

"Process" or "processing" means any collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

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

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Protected health information" has the meaning ascribed thereto in 45 C.F.R. § 160.103.

"Publicly available information" means information that is lawfully made available from federal, state, or local government records.

"Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

"Sale," "sell," or "sold" means the exchange of personal data for monetary consideration by a controller to a third party for purposes of licensing or selling personal data at the third party's discretion to additional third parties. "Sale" does not include (i) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) 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 (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation; (ii) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; or (ii) the personal data of an individual known to be a child.

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected on the basis of personal data obtained or inferred over time from a consumer's activities across nonaffiliated web sites, applications, or online services to predict user preferences or interests. "Targeted advertising" does not include advertising to a consumer on the bas is of the consumer's visits to a website, application, or online service that a reasonable consumer would believe to be associated with the publisher where the advertisement is placed on the basis of common branding, trademarks, or other indicia of common ownership or in response to the consumer's request for information or feedback.

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

"Verified request" means the process through which a consumer may submit a request to exercise a right or rights set forth in this chapter and by which a controller can reasonably authenticate the request and the consumer making the request using commercially reasonable means.

§ 59.1-572. Scope of chapter.

A. This chapter applies to any legal entity (i) that conducts business in the Commonwealth or produces products or services that are intentionally targeted to residents of the Commonwealth and (ii) that:

1. Controls or processes personal data of not fewer than 100,000 consumers; or

2. Derives over 50 percent of gross revenue from the sale of personal data and processes or controls personal data of not fewer than 25,000 customers.

B. This chapter does not apply to:

1. State governments;

2. County, city, or town governments or local school boards;

3. Information that meets the definition of:

a. Protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., and related regulations;

b. Health care information;

c. Patient identifying information for purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. § 290 dd-2;

d. Identifiable private information for purposes of 45 C.F.R. Part 46;

e. Information and documents created specifically for, and collected and maintained by:

(1) A quality improvement committee;

(2) A peer review committee;

(3) A quality assurance committee;

(4) A hospital for reporting of health care-associated infections;

(5) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. § 1101 et seq., and related regulations; or

(6) Patient safety work product information for purposes of 42 C.F.R. Part 3, established pursuant to 42 U.S.C. § 299b-21-26;

4. Information maintained in the same manner as information under subdivision 3 by:

a. A covered entity or business associate as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., and related regulations;

b. A health care facility or health care provider; or

c. A program or a qualified service organization as defined by 42 C.F.R. Part 2, established

pursuant to 42 U.S.C. Sec. 290 dd-2;

5. Personal data provided to or from, or held by, a consumer reporting agency as defined by 15 U.S.C. § 1681a(f), provided that use of that data is in compliance with the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.;

6. Personal data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, P.L. 106-102, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with such act;

7. Personal data collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. §. 2721 et seq., if the collection, processing, sale, or disclosure is in compliance with such act; or

8. Data maintained for employment records purposes.

§ 59.1-573. Responsibility according to role.

A. Controllers are responsible for meeting the obligations established under this chapter.

B. Processors are responsible under this chapter for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter.

C. Processing by a processor is governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

§ 59.1-574. Consumer rights.

A. Controllers shall facilitate verified requests to exercise the following consumer rights:

1. Upon a verified request from a consumer, a controller shall confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data that the controller maintains in identifiable form concerning the consumer. Upon a verified request from a consumer, a controller shall provide a copy of the personal data that the controller maintains in identifiable form undergoing processing. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information shall be provided in a commonly used electronic form. This subdivision does not adversely affect the rights or freedoms of others.

2. Upon a verified request from a consumer, the controller, without undue delay, shall correct inaccurate personal data that the controller maintains in identifiable form concerning the consumer. Taking into account the business purposes of the processing, the controller shall complete incomplete personal data, including by means of providing a supplementary statement where appropriate.

3. Upon a verified request from a consumer, a controller shall delete, without undue delay, the consumer's personal data that the controller maintains in identifiable form if (i) the personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer; (ii) for processing that requires consent, the consumer withdraws consent to processing and there are no business purposes for the processing; (iii) the consumer objects to the processing pursuant to subdivision 6 and (a) there are no business purposes for processing the personal data for the controller, the consumer whose personal data is being processed, or the public for which such processing is necessary or (b) the processing is for targeted advertising; (iv) the personal data has been unlawfully processed; or (v) the personal data shall be deleted to comply with a legal obligation under federal, state, or local law to which the controller is subject.

4. Upon a verified request from a consumer, the controller shall restrict processing of personal data that the controller maintains in identifiable form if the purpose for which the personal data is (i) not consistent with a purpose for which the personal data was collected, (ii) not consistent with a purpose disclosed to the consumer at the time of collection or authorization, or (iii) unlawful. Where personal data is subject to a restriction of processing under this subdivision, the personal data shall, with the exception of storage, be processed only (a) with the consumer's consent; (b) for the establishment, exercise, or defense of legal claims; (c) for the protection of the rights of another natural or legal person; (d) for reasons of important public interest under federal, state, or local law; (e) to provide products or services requested by the consumer; or (f) for another purpose set forth in subdivision 3. A consumer who has obtained restriction of processing pursuant to this subdivision shall be informed by the controller before the restriction of processing is lifted.

5. Upon a verified request from a consumer, the controller shall provide to the consumer, if technically feasible and commercially reasonable, any personal data that the controller maintains in identifiable form concerning the consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i) the processing of such personal data requires consent under subsection C of § 59.1-576, the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or in order to take steps at the request of the consumer prior to entering into a contract and (ii) the processing is carried out by automated

means. Requests for personal data under this subdivision shall be without prejudice to the other rights granted in this chapter. The rights provided in this subdivision do not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and shall not adversely affect the rights of others.

6. A consumer may object through a verified request, on grounds relating to the consumer's particular situation, at any time to processing of personal data concerning such consumer. When a consumer objects to the processing of the consumer's personal data for targeted advertising, which includes the sale of personal data concerning the consumer to third parties for purposes of targeted advertising, the controller shall no longer process the personal data subject to the objection for such purpose and shall take reasonable steps to communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for such purposes to any third parties to whom the controller sold the consumer's personal data for such purposes. Third parties shall honor objection requests pursuant to this subdivision received from third-party controllers. If a consumer objects to processing for any purpose, other than targeted advertising, the controller may continue processing the personal data subject to the objection if (i) the controller demonstrates a legitimate ground to process such personal data that overrides the potential risks to the rights of the consumer associated with the processing or (ii) another exemption in this chapter applies.

B. A controller shall communicate any correction, deletion, or restriction of processing carried out in accordance with subdivision A 2, 3, or 4 to each third-party recipient to whom the controller knows the personal data has been disclosed, including third parties that received the data through a sale, within one year preceding the verified request unless (i) such communication proves functionally impractical or technically infeasible or involves disproportionate effort or (ii) the controller knows or is informed by the third party that the third party is not continuing to use the personal data. The controller shall inform the consumer about third-party recipients or categories with whom the controller shares personal information, if any, if the consumer requests such information.

C. A controller shall provide information on action taken on a verified request under subdivisions A 1 through 6 without undue delay and in any event within 30 days of receipt of the request. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of any such extension within 30 days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the consumer. If a controller does not take action on the request of a consumer, the controller shall inform the consumer without undue delay and at the latest within 30 days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller. Information provided under this section shall be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request. Where the controller has reasonable doubts concerning the identity of the consumer making a request under subdivisions A 1 through 6, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

§ 59.1-575. Transparency.

A. Controllers shall be transparent and accountable for their processing of personal data by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that includes:

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

2. The purposes for which the categories of personal data are used and disclosed to third parties, if any;

3. The rights that consumers may exercise pursuant to § 59.1-574, if any;

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.

B. If a controller sells personal data to data brokers or processes personal data for targeted advertising, it shall disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and conspicuous manner.

§ 59.1-576. Risk assessments.

A. Controllers shall conduct, to the extent not previously conducted, a risk assessment of each of their processing activities involving personal data and an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. Such risk assessments shall take

into account the type of personal data to be processed by the controller, including the extent to which the personal data is sensitive data or otherwise sensitive in nature and the context in which the personal data is to be processed.

B. Risk assessments conducted under subsection A shall identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, 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 deidentified 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 factor into this assessment by the controller.

C. If the risk assessment conducted under subsection A determines that the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer or if another exemption under this chapter applies. To the extent that the controller seeks consumer consent for processing, such consent shall be as easy to withdraw as to give.

D. Processing for a business purpose shall be presumed to be permissible unless (i) it involves the processing of sensitive data and (ii) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.

E. The controller shall make the risk assessment available to the Attorney General upon request. Risk assessments are confidential and exempt from mandatory disclosure under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).

§ 59.1-577. Deidentified data.

A controller or processor that uses deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject and shall take appropriate steps to address any breaches of contractual commitments.

§ 59.1-578. Exempt actions.

A. The obligations imposed on controllers or processors under this chapter do not 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 law;

4. Investigate, exercise, or defend legal claims;

5. Prevent or detect identity theft, fraud, or other criminal activity or verify identities;

6. Enter into a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

7. Protect the vital interests of the consumer or of another individual;

8. Perform a task carried out in the public interest or in the exercise of official authority vested in the controller;

9. Process personal data of a consumer for one or more specific purposes where the consumer has consented in writing to the processing; or

10. Prevent, detect, 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.

B. The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under applicable law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under applicable law as part of a privileged communication.

C. 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, including under § 59.1-579, if the recipient processes such personal data 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 is likewise not liable under this chapter, including under § 59.1-579, for the obligations of a controller or processor to which it provides services.

D. This chapter does not require a controller or processor to do the following:

1. Reidentify deidentified data;

2. Retain, link, or combine personal data concerning a consumer that it would not otherwise retain,

link, or combine in the ordinary course of business; or

3. Comply with a request to exercise any of the rights under subdivisions A 1 through 6 of § 59.1-574 if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

E. Obligations imposed on controllers and processors under this chapter do not:

1. Adversely affect the rights or freedoms of any persons; or

2. Apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

§ 59.1-579. Violation of chapter; liability.

A. A controller or processor is in violation of this chapter if it fails to cure any alleged violation of this chapter within 30 days after receiving notice of alleged noncompliance.

B. Any violation of the provisions of this chapter shall constitute a prohibited practice pursuant to the provisions of § 59.1-200 and shall be subject to any and all of the enforcement provisions of the Virginia Consumer Protection Act (§ 59.1-196 et seq.).

C. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.