

24104993D

HOUSE BILL NO. 707

Offered January 10, 2024

Prefiled January 9, 2024

A BILL to amend and reenact §§ 59.1-578 and 59.1-580 of the Code of Virginia, relating to Consumer Data Protection Act; protections for children.

Patrons—Maldonado, Cherry, Sewell and Sullivan; Senator: Aird

Referred to Committee on Labor and Commerce

Be it enacted by the General Assembly of Virginia:**1. That §§ 59.1-578 and 59.1-580 of the Code of Virginia are amended and reenacted as follows:****§ 59.1-578. Data controller responsibilities; transparency.****A. A controller shall:**

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

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

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

4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-577 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program;

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. No controller shall process personal data of a known child:

1. For the purposes of (i) targeted advertising, (ii) the sale of such personal data, or (iii) profiling in

59 furtherance of decisions that produce legal or similarly significant effects concerning a consumer;

60 2. For any processing purpose other than the processing purpose that the controller disclosed at the
61 time such controller collected such personal data or that is reasonably necessary for and compatible
62 with such disclosed purpose, unless such processing is reasonably necessary to provide an online
63 service, product, or feature. If such processing is reasonably necessary to provide an online service,
64 product, or feature, such controller shall only process such data for the time necessary to provide such
65 online service, product, or feature; or

66 3. For any processing purpose without first obtaining consent from the child's parent or legal
67 guardian in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et
68 seq.).

69 G. No controller shall collect precise geolocation data from a known child unless (i) such precise
70 geolocation data is reasonably necessary for the controller to provide an online service, product, or
71 feature and, if such data is necessary to provide such online service, product, or feature, such controller
72 shall only collect such data for the time necessary to provide such online service, product, or feature;
73 (ii) the controller provides to the known child a signal indicating that such controller is collecting such
74 precise geolocation data, which signal shall be available to such known child for the entire duration of
75 such collection; and (iii) the controller obtains consent from the child's parent or legal guardian in
76 accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

77 **§ 59.1-580. Data protection assessments.**

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

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

81 2. The sale of personal data;

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

87 4. The processing of sensitive data; and

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

90 B. Each controller that, on or after January 1, 2025, offers any online service, product, or feature
91 directed to consumers whom such controller has actual knowledge are children shall conduct a data
92 protection assessment for such online service, product, or feature that addresses (i) the purpose of such
93 online service, product, or feature; (ii) the categories of known children's personal data that such online
94 service, product, or feature processes; and (iii) the purposes for which such controller processes known
95 children's personal data with respect to such online service, product, or feature.

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

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

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

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

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