1   **VIRGINIA ACTS OF ASSEMBLY — CHAPTER**

2   *An Act to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 52, consisting of*
3   *sections numbered 59.1-571 through 59.1-581, relating to Consumer Data Protection Act.*

                                                      [H 2307]

4
5   Approved

6   **Be it enacted by the General Assembly of Virginia:**
7   **1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 52, consisting**
8   **of sections numbered 59.1-571 through 59.1-581, as follows:**
9   *CHAPTER 52.*
10   *CONSUMER DATA PROTECTION ACT.*
11   *§ 59.1-571. Definitions.*
12   *As used in this chapter, unless the context requires a different meaning:*
13   *"Affiliate" means a legal entity that controls, is controlled by, or is under common control with*
14   *another legal entity or shares common branding with another legal entity. For the purposes of this*
15   *definition, "control" or "controlled" means (i) ownership of, or the power to vote, more than 50 percent*
16   *of the outstanding shares of any class of voting security of a company; (ii) control in any manner over*
17   *the election of a majority of the directors or of individuals exercising similar functions; or (iii) the*
18   *power to exercise controlling influence over the management of a company.*
19   *"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his*
20   *consumer rights in § 59.1-573, is the same consumer exercising such consumer rights with respect to the*
21   *personal data at issue.*
22   *"Biometric data" means data generated by automatic measurements of an individual's biological*
23   *characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns*
24   *or characteristics that is used to identify a specific individual. "Biometric data" does not include a*
25   *physical or digital photograph, a video or audio recording or data generated therefrom, or information*
26   *collected, used, or stored for health care treatment, payment, or operations under HIPAA.*
27   *"Business associate" means the same meaning as the term established by HIPAA.*
28   *"Child" means any natural person younger than 13 years of age.*
29   *"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and*
30   *unambiguous agreement to process personal data relating to the consumer. Consent may include a*
31   *written statement, including a statement written by electronic means, or any other unambiguous*
32   *affirmative action.*
33   *"Consumer" means a natural person who is a resident of the Commonwealth acting only in an*
34   *individual or household context. It does not include a natural person acting in a commercial or*
35   *employment context.*
36   *"Controller" means the natural or legal person that, alone or jointly with others, determines the*
37   *purpose and means of processing personal data.*
38   *"Covered entity" means the same as the term is established by HIPAA.*
39   *"Decisions that produce legal or similarly significant effects concerning a consumer" means a*
40   *decision made by the controller that results in the provision or denial by the controller of financial and*
41   *lending services, housing, insurance, education enrollment, criminal justice, employment opportunities,*
42   *health care services, or access to basic necessities, such as food and water.*
43   *"De-identified data" means data that cannot reasonably be linked to an identified or identifiable*
44   *natural person, or a device linked to such person. A controller that possesses "de-identified data" shall*
45   *comply with the requirements of subsection A of § 59.1-577.*
46   *"Fund" means the Consumer Privacy Fund established pursuant to § 59.1-581.*
47   *"Health record" means the same as that term is defined in § 32.1-127.1:03.*
48   *"Health care provider" means the same as that term is defined in § 32.1-276.3.*
49   *"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C.*
50   *§ 1320d et seq.).*
51   *"Identified or identifiable natural person" means a person who can be readily identified, directly or*
52   *indirectly.*
53   *"Institution of higher education" means a public institution and private institution of higher*
54   *education, as those terms are defined in § 23.1-100.*
55   *"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation*
56   *Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3), 501(c)(6), or 501*

57 *(c)(12) of the Internal Revenue Code, and any subsidiaries and affiliates of entities organized pursuant*
58 *to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.*
59 *"Personal data" means any information that is linked or reasonably linkable to an identified or*
60 *identifiable natural person. "Personal data" does not include de-identified data or publicly available*
61 *information.*
62 *"Precise geolocation data" means information derived from technology, including but not limited to*
63 *global positioning system level latitude and longitude coordinates or other mechanisms, that directly*
64 *identifies the specific location of a natural person with precision and accuracy within a radius of 1,750*
65 *feet. "Precise geolocation data" does not include the content of communications or any data generated*
66 *by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.*
67 *"Process" or "processing" means any operation or set of operations performed, whether by manual*
68 *or automated means, on personal data or on sets of personal data, such as the collection, use, storage,*
69 *disclosure, analysis, deletion, or modification of personal data.*
70 *"Processor" means a natural or legal entity that processes personal data on behalf of a controller.*
71 *"Profiling" means any form of automated processing performed on personal data to evaluate,*
72 *analyze, or predict personal aspects related to an identified or identifiable natural person's economic*
73 *situation, health, personal preferences, interests, reliability, behavior, location, or movements.*
74 *"Protected health information" means the same as the term is established by HIPAA.*
75 *"Pseudonymous data" means personal data that cannot be attributed to a specific natural person*
76 *without the use of additional information, provided that such additional information is kept separately*
77 *and is subject to appropriate technical and organizational measures to ensure that the personal data is*
78 *not attributed to an identified or identifiable natural person.*
79 *"Publicly available information" means information that is lawfully made available through federal,*
80 *state, or local government records, or information that a business has a reasonable basis to believe is*
81 *lawfully made available to the general public through widely distributed media, by the consumer, or by*
82 *a person to whom the consumer has disclosed the information, unless the consumer has restricted the*
83 *information to a specific audience.*
84 *"Sale of personal data" means the exchange of personal data for monetary consideration by the*
85 *controller to a third party. "Sale of personal data" does not include:*
86 *1. The disclosure of personal data to a processor that processes the personal data on behalf of the*
87 *controller;*
88 *2. The disclosure of personal data to a third party for purposes of providing a product or service*
89 *requested by the consumer;*
90 *3. The disclosure or transfer of personal data to an affiliate of the controller;*
91 *4. The disclosure of information that the consumer (i) intentionally made available to the general*
92 *public via a channel of mass media and (ii) did not restrict to a specific audience; or*
93 *5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger,*
94 *acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of*
95 *the controller's assets.*
96 *"Sensitive data" means a category of personal data that includes:*
97 *1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health*
98 *diagnosis, sexual orientation, or citizenship or immigration status;*
99 *2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural*
100 *person;*
101 *3. The personal data collected from a known child; or*
102 *4. Precise geolocation data.*
103 *"State agency" means the same as that term is defined in § 2.2-307.*
104 *"Targeted advertising" means displaying advertisements to a consumer where the advertisement is*
105 *selected based on personal data obtained from that consumer's activities over time and across*
106 *nonaffiliated websites or online applications to predict such consumer's preferences or interests.*
107 *"Targeted advertising" does not include:*
108 *1. Advertisements based on activities within a controller's own websites or online applications;*
109 *2. Advertisements based on the context of a consumer's current search query, visit to a website, or*
110 *online application;*
111 *3. Advertisements directed to a consumer in response to the consumer's request for information or*
112 *feedback; or*
113 *4. Processing personal data processed solely for measuring or reporting advertising performance,*
114 *reach, or frequency.*
115 *"Third party" means a natural or legal person, public authority, agency, or body other than the*
116 *consumer, controller, processor, or an affiliate of the processor or the controller.*
117 *§ 59.1-572. Scope; exemptions.*

118   *A. This chapter applies to persons that conduct business in the Commonwealth or produce products*
119 *or services that are targeted to residents of the Commonwealth and that (i) during a calendar year,*
120 *control or process personal data of at least 100,000 consumers or (ii) control or process personal data*
121 *of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal*
122 *data.*
123   *B. This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or*
124 *agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial*
125 *institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);*
126 *(iii) covered entity or business associate governed by the privacy, security, and breach notification rules*
127 *issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established*
128 *pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L.*
129 *111-5); (iv) nonprofit organization; or (v) institution of higher education.*
130   *C. The following information and data is exempt from this chapter:*
131   *1. Protected health information under HIPAA;*
132   *2. Health records for purposes of Title 32.1;*
133   *3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;*
134   *4. Identifiable private information for purposes of the federal policy for the protection of human*
135 *subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected*
136 *as part of human subjects research pursuant to the good clinical practice guidelines issued by The*
137 *International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human*
138 *Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or*
139 *shared in research conducted in accordance with the requirements set forth in this chapter, or other*
140 *research conducted in accordance with applicable law;*
141   *5. Information and documents created for purposes of the federal Health Care Quality Improvement*
142 *Act of 1986 (42 U.S.C. § 11101 et seq.);*
143   *6. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement*
144 *Act (42 U.S.C. § 299b-21 et seq.);*
145   *7. Information derived from any of the health care-related information listed in this subsection that is*
146 *de-identified in accordance with the requirements for de-identification pursuant to HIPAA;*
147   *8. Information originating from, and intermingled to be indistinguishable with, or information treated*
148 *in the same manner as information exempt under this subsection that is maintained by a covered entity*
149 *or business associate as defined by HIPAA or a program or a qualified service organization as defined*
150 *by 42 U.S.C. § 290dd-2;*
151   *9. Information used only for public health activities and purposes as authorized by HIPAA;*
152   *10. The collection, maintenance, disclosure, sale, communication, or use of any personal information*
153 *bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general*
154 *reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that*
155 *provides information for use in a consumer report, and by a user of a consumer report, but only to the*
156 *extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15*
157 *U.S.C. § 1681 et seq.);*
158   *11. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's*
159 *Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);*
160   *12. Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C.*
161 *§ 1232g et seq.);*
162   *13. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit*
163 *Act (12 U.S.C. § 2001 et seq.); and*
164   *14. Data processed or maintained (i) in the course of an individual applying to, employed by, or*
165 *acting as an agent or independent contractor of a controller, processor, or third party, to the extent that*
166 *the data is collected and used within the context of that role; (ii) as the emergency contact information*
167 *of an individual under this chapter used for emergency contact purposes; or (iii) that is necessary to*
168 *retain to administer benefits for another individual relating to the individual under clause (i) and used*
169 *for the purposes of administering those benefits.*
170   *D. Controllers and processors that comply with the verifiable parental consent requirements of the*
171 *Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any*
172 *obligation to obtain parental consent under this chapter.*
173   **§ 59.1-573. Personal data rights; consumers.**
174   *A. A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by*
175 *submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A*
176 *known child's parent or legal guardian may invoke such consumer rights on behalf of the child*
177 *regarding processing personal data belonging to the known child. A controller shall comply with an*
178 *authenticated consumer request to exercise the right:*

179 *1. To confirm whether or not a controller is processing the consumer's personal data and to access*
180 *such personal data;*
181 *2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the*
182 *personal data and the purposes of the processing of the consumer's personal data;*
183 *3. To delete personal data provided by or obtained about the consumer;*
184 *4. To obtain a copy of the consumer's personal data that the consumer previously provided to the*
185 *controller in a portable and, to the extent technically feasible, readily usable format that allows the*
186 *consumer to transmit the data to another controller without hindrance, where the processing is carried*
187 *out by automated means; and*
188 *5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the*
189 *sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly*
190 *significant effects concerning the consumer.*
191 *B. Except as otherwise provided in this chapter, a controller shall comply with a request by a*
192 *consumer to exercise the consumer rights authorized pursuant to subsection A as follows:*
193 *1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of*
194 *receipt of the request submitted pursuant to the methods described in § 59.1-573 A. The response period*
195 *may be extended once by 45 additional days when reasonably necessary, taking into account the*
196 *complexity and number of the consumer's requests, so long as the controller informs the consumer of*
197 *any such extension within the initial 45-day response period, together with the reason for the extension.*
198 *2. If a controller declines to take action regarding the consumer's request, the controller shall inform*
199 *the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the*
200 *request, of the justification for declining to take action and instructions for how to appeal the decision*
201 *pursuant to subsection C.*
202 *3. Information provided in response to a consumer request shall be provided by a controller free of*
203 *charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded,*
204 *excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the*
205 *administrative costs of complying with the request or decline to act on the request. The controller bears*
206 *the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.*
207 *4. If a controller is unable to authenticate the request using commercially reasonable efforts, the*
208 *controller shall not be required to comply with a request to initiate an action under subsection A and*
209 *may request that the consumer provide additional information reasonably necessary to authenticate the*
210 *consumer and the consumer's request.*
211 *C. A controller shall establish a process for a consumer to appeal the controller's refusal to take*
212 *action on a request within a reasonable period of time after the consumer's receipt of the decision*
213 *pursuant to subdivision B 2. The appeal process shall be conspicuously available and similar to the*
214 *process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of*
215 *an appeal, a controller shall inform the consumer in writing of any action taken or not taken in*
216 *response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is*
217 *denied, the controller shall also provide the consumer with an online mechanism, if available, or other*
218 *method through which the consumer may contact the Attorney General to submit a complaint.*
219 *§ 59.1-574. Data controller responsibilities; transparency.*
220 *A. A controller shall:*
221 *1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in*
222 *relation to the purposes for which such data is processed, as disclosed to the consumer;*
223 *2. Except as otherwise provided in this chapter, not process personal data for purposes that are*
224 *neither reasonably necessary to nor compatible with the disclosed purposes for which such personal*
225 *data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;*
226 *3. Establish, implement, and maintain reasonable administrative, technical, and physical data*
227 *security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data*
228 *security practices shall be appropriate to the volume and nature of the personal data at issue;*
229 *4. Not process personal data in violation of state and federal laws that prohibit unlawful*
230 *discrimination against consumers. A controller shall not discriminate against a consumer for exercising*
231 *any of the consumer rights contained in this chapter, including denying goods or services, charging*
232 *different prices or rates for goods or services, or providing a different level of quality of goods and*
233 *services to the consumer. However, nothing in this subdivision shall be construed to require a controller*
234 *to provide a product or service that requires the personal data of a consumer that the controller does*
235 *not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or*
236 *selection of goods or services to a consumer, including offering goods or services for no fee, if the*
237 *consumer has exercised his right to opt out pursuant to § 59.1-573 or the offer is related to a*
238 *consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club*
239 *card program; and*

240   *5. Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in*
241 *the case of the processing of sensitive data concerning a known child, without processing such data in*
242 *accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).*
243   *B. Any provision of a contract or agreement of any kind that purports to waive or limit in any way*
244 *consumer rights pursuant to § 59.1-573 shall be deemed contrary to public policy and shall be void and*
245 *unenforceable.*
246   *C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy*
247 *notice that includes:*
248   *1. The categories of personal data processed by the controller;*
249   *2. The purpose for processing personal data;*
250   *3. How consumers may exercise their consumer rights pursuant § 59.1-573, including how a*
251 *consumer may appeal a controller's decision with regard to the consumer's request;*
252   *4. The categories of personal data that the controller shares with third parties, if any; and*
253   *5. The categories of third parties, if any, with whom the controller shares personal data.*
254   *D. If a controller sells personal data to third parties or processes personal data for targeted*
255 *advertising, the controller shall clearly and conspicuously disclose such processing, as well as the*
256 *manner in which a consumer may exercise the right to opt out of such processing.*
257   *E. A controller shall establish, and shall describe in a privacy notice, one or more secure and*
258 *reliable means for consumers to submit a request to exercise their consumer rights under this chapter.*
259 *Such means shall take into account the ways in which consumers normally interact with the controller,*
260 *the need for secure and reliable communication of such requests, and the ability of the controller to*
261 *authenticate the identity of the consumer making the request. Controllers shall not require a consumer*
262 *to create a new account in order to exercise consumer rights pursuant to § 59.1-573 but may require a*
263 *consumer to use an existing account.*
264   *§ 59.1-575. Responsibility according to role; controller and processor.*
265   *A. A processor shall adhere to the instructions of a controller and shall assist the controller in*
266 *meeting its obligations under this chapter. Such assistance shall include:*
267   *1. Taking into account the nature of processing and the information available to the processor, by*
268 *appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill*
269 *the controller's obligation to respond to consumer rights requests pursuant to § 59.1-573.*
270   *2. Taking into account the nature of processing and the information available to the processor, by*
271 *assisting the controller in meeting the controller's obligations in relation to the security of processing*
272 *the personal data and in relation to the notification of a breach of security of the system of the*
273 *processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.*
274   *3. Providing necessary information to enable the controller to conduct and document data protection*
275 *assessments pursuant to § 59.1-576.*
276   *B. A contract between a controller and a processor shall govern the processor's data processing*
277 *procedures with respect to processing performed on behalf of the controller. The contract shall be*
278 *binding and clearly set forth instructions for processing data, the nature and purpose of processing, the*
279 *type of data subject to processing, the duration of processing, and the rights and obligations of both*
280 *parties. The contract shall also include requirements that the processor shall:*
281   *1. Ensure that each person processing personal data is subject to a duty of confidentiality with*
282 *respect to the data;*
283   *2. At the controller's direction, delete or return all personal data to the controller as requested at*
284 *the end of the provision of services, unless retention of the personal data is required by law;*
285   *3. Upon the reasonable request of the controller, make available to the controller all information in*
286 *its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;*
287   *4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated*
288 *assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct*
289 *an assessment of the processor's policies and technical and organizational measures in support of the*
290 *obligations under this chapter using an appropriate and accepted control standard or framework and*
291 *assessment procedure for such assessments. The processor shall provide a report of such assessment to*
292 *the controller upon request; and*
293   *5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that*
294 *requires the subcontractor to meet the obligations of the processor with respect to the personal data.*
295   *C. Nothing in this section shall be construed to relieve a controller or a processor from the*
296 *liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.*
297   *D. Determining whether a person is acting as a controller or processor with respect to a specific*
298 *processing of data is a fact-based determination that depends upon the context in which personal data is*
299 *to be processed. A processor that continues to adhere to a controller's instructions with respect to a*
300 *specific processing of personal data remains a processor.*

301 **§ 59.1-576. Data protection assessments.**
302 *A. A controller shall conduct and document a data protection assessment of each of the following*
303 *processing activities involving personal data:*
304 *1. The processing of personal data for purposes of targeted advertising;*
305 *2. The sale of personal data;*
306 *3. The processing of personal data for purposes of profiling, where such profiling presents a*
307 *reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on,*
308 *consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other*
309 *intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such*
310 *intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;*
311 *4. The processing of sensitive data; and*
312 *5. Any processing activities involving personal data that present a heightened risk of harm to*
313 *consumers.*
314 *B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the*
315 *benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other*
316 *stakeholders, and the public against the potential risks to the rights of the consumer associated with*
317 *such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.*
318 *The use of de-identified data and the reasonable expectations of consumers, as well as the context of the*
319 *processing and the relationship between the controller and the consumer whose personal data will be*
320 *processed, shall be factored into this assessment by the controller.*
321 *C. The Attorney General may request, pursuant to a civil investigative demand, that a controller*
322 *disclose any data protection assessment that is relevant to an investigation conducted by the Attorney*
323 *General, and the controller shall make the data protection assessment available to the Attorney General.*
324 *The Attorney General may evaluate the data protection assessment for compliance with the*
325 *responsibilities set forth in § 59.1-574. Data protection assessments shall be confidential and exempt*
326 *from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).*
327 *The disclosure of a data protection assessment pursuant to a request from the Attorney General shall*
328 *not constitute a waiver of attorney-client privilege or work product protection with respect to the*
329 *assessment and any information contained in the assessment.*
330 *D. A single data protection assessment may address a comparable set of processing operations that*
331 *include similar activities.*
332 *E. Data protection assessments conducted by a controller for the purpose of compliance with other*
333 *laws or regulations may comply under this section if the assessments have a reasonably comparable*
334 *scope and effect.*
335 *F. Data protection assessment requirements shall apply to processing activities created or generated*
336 *after January 1, 2023, and are not retroactive.*
337 **§ 59.1-577. Processing de-identified data; exemptions.**
338 *A. The controller in possession of de-identified data shall:*
339 *1. Take reasonable measures to ensure that the data cannot be associated with a natural person;*
340 *2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the*
341 *data; and*
342 *3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this*
343 *chapter.*
344 *B. Nothing in this chapter shall be construed to (i) require a controller or processor to re-identify*
345 *de-identified data or pseudonymous data or (ii) maintain data in identifiable form, or collect, obtain,*
346 *retain, or access any data or technology, in order to be capable of associating an authenticated*
347 *consumer request with personal data.*
348 *C. Nothing in this chapter shall be construed to require a controller or processor to comply with an*
349 *authenticated consumer rights request, pursuant to § 59.1-573, if all of the following are true:*
350 *1. The controller is not reasonably capable of associating the request with the personal data or it*
351 *would be unreasonably burdensome for the controller to associate the request with the personal data;*
352 *2. The controller does not use the personal data to recognize or respond to the specific consumer*
353 *who is the subject of the personal data, or associate the personal data with other personal data about*
354 *the same specific consumer; and*
355 *3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose*
356 *the personal data to any third party other than a processor, except as otherwise permitted in this*
357 *section.*
358 *D. The consumer rights contained in subdivisions A 1 through 4 of § 59.1-573 and § 59.1-574 shall*
359 *not apply to pseudonymous data in cases where the controller is able to demonstrate any information*
360 *necessary to identify the consumer is kept separately and is subject to effective technical and*
361 *organizational controls that prevent the controller from accessing such information.*

362   *E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable*
363 *oversight to monitor compliance with any contractual commitments to which the pseudonymous data or*
364 *de-identified data is subject and shall take appropriate steps to address any breaches of those*
365 *contractual commitments.*
366   **§ 59.1-578. Limitations.**
367   *A. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:*
368   *1. Comply with federal, state, or local laws, rules, or regulations;*
369   *2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by*
370 *federal, state, local, or other governmental authorities;*
371   *3. Cooperate with law-enforcement agencies concerning conduct or activity that the controller or*
372 *processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or*
373 *regulations;*
374   *4. Investigate, establish, exercise, prepare for, or defend legal claims;*
375   *5. Provide a product or service specifically requested by a consumer, perform a contract to which*
376 *the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request*
377 *of the consumer prior to entering into a contract;*
378   *6. Take immediate steps to protect an interest that is essential for the life or physical safety of the*
379 *consumer or of another natural person, and where the processing cannot be manifestly based on*
380 *another legal basis;*
381   *7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment,*
382 *malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or*
383 *investigate, report, or prosecute those responsible for any such action;*
384   *8. Engage in public or peer-reviewed scientific or statistical research in the public interest that*
385 *adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an*
386 *institutional review board, or similar independent oversight entities that determine: (i) if the deletion of*
387 *the information is likely to provide substantial benefits that do not exclusively accrue to the controller;*
388 *(ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has*
389 *implemented reasonable safeguards to mitigate privacy risks associated with research, including any*
390 *risks associated with reidentification; or*
391   *9. Assist another controller, processor, or third party with any of the obligations under this*
392 *subsection.*
393   *B. The obligations imposed on controllers or processors under this chapter shall not restrict a*
394 *controller's or processor's ability to collect, use, or retain data to:*
395   *1. Conduct internal research to develop, improve, or repair products, services, or technology;*
396   *2. Effectuate a product recall;*
397   *3. Identify and repair technical errors that impair existing or intended functionality; or*
398   *4. Perform internal operations that are reasonably aligned with the expectations of the consumer or*
399 *reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise*
400 *compatible with processing data in furtherance of the provision of a product or service specifically*
401 *requested by a consumer or the performance of a contract to which the consumer is a party.*
402   *C. The obligations imposed on controllers or processors under this chapter shall not apply where*
403 *compliance by the controller or processor with this chapter would violate an evidentiary privilege under*
404 *the laws of the Commonwealth. Nothing in this chapter shall be construed to prevent a controller or*
405 *processor from providing personal data concerning a consumer to a person covered by an evidentiary*
406 *privilege under the laws of the Commonwealth as part of a privileged communication.*
407   *D. A controller or processor that discloses personal data to a third-party controller or processor, in*
408 *compliance with the requirements of this chapter, is not in violation of this chapter if the third-party*
409 *controller or processor that receives and processes such personal data is in violation of this chapter,*
410 *provided that, at the time of disclosing the personal data, the disclosing controller or processor did not*
411 *have actual knowledge that the recipient intended to commit a violation. A third-party controller or*
412 *processor receiving personal data from a controller or processor in compliance with the requirements of*
413 *this chapter is likewise not in violation of this chapter for the transgressions of the controller or*
414 *processor from which it receives such personal data.*
415   *E. Nothing in this chapter shall be construed as an obligation imposed on controllers and processors*
416 *that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech*
417 *pursuant to the First Amendment to the United States Constitution, or applies to the processing of*
418 *personal data by a person in the course of a purely personal or household activity.*
419   *F. Personal data processed by a controller pursuant to this section shall not be processed for any*
420 *purpose other than those expressly listed in this section unless otherwise allowed by this chapter.*
421 *Personal data processed by a controller pursuant to this section may be processed to the extent that*
422 *such processing is:*

423   *1. Reasonably necessary and proportionate to the purposes listed in this section; and*
424   *2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in*
425   *this section. Personal data collected, used, or retained pursuant to subsection B shall, where applicable,*
426   *take into account the nature and purpose or purposes of such collection, use, or retention. Such data*
427   *shall be subject to reasonable administrative, technical, and physical measures to protect the*
428   *confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable*
429   *risks of harm to consumers relating to such collection, use, or retention of personal data.*
430   *G. If a controller processes personal data pursuant to an exemption in this section, the controller*
431   *bears the burden of demonstrating that such processing qualifies for the exemption and complies with*
432   *the requirements in subsection F.*
433   *H. Processing personal data for the purposes expressly identified in subdivisions A 1 through 9 shall*
434   *not solely make an entity a controller with respect to such processing.*
435   ***§ 59.1-579. Investigative authority.***
436   *Whenever the Attorney General has reasonable cause to believe that any person has engaged in, is*
437   *engaging in, or is about to engage in any violation of this chapter, the Attorney General is empowered*
438   *to issue a civil investigative demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil*
439   *investigative demands issued under this section.*
440   ***§ 59.1-580. Enforcement; civil penalty; expenses.***
441   *A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.*
442   *B. Prior to initiating any action under this chapter, the Attorney General shall provide a controller*
443   *or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney*
444   *General alleges have been or are being violated. If within the 30-day period, the controller or processor*
445   *cures the noticed violation and provides the Attorney General an express written statement that the*
446   *alleged violations have been cured and that no further violations shall occur, no action shall be*
447   *initiated against the controller or processor.*
448   *C. If a controller or processor continues to violate this chapter following the cure period in*
449   *subsection B or breaches an express written statement provided to the Attorney General under that*
450   *subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek*
451   *an injunction to restrain any violations of this chapter and civil penalties of up to $7,500 for each*
452   *violation under this chapter.*
453   *D. The Attorney General may recover reasonable expenses incurred in investigating and preparing*
454   *the case, including attorney fees, in any action initiated under this chapter.*
455   *E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private*
456   *right of action for violations of this chapter or under any other law.*
457   ***§ 59.1-581. Consumer Privacy Fund.***
458   *There is hereby created in the state treasury a special nonreverting fund to be known as the*
459   *Consumer Privacy Fund. The Fund shall be established on the books of the Comptroller. All civil*
460   *penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state*
461   *treasury and credited to the Fund. Interest earned on moneys in the Fund shall remain in the Fund and*
462   *be credited to it. Any moneys remaining in the Fund, including interest thereon, at the end of each*
463   *fiscal year shall not revert to the general fund but shall remain in the Fund. Moneys in the Fund shall*
464   *be used to support the work of the Office of the Attorney General to enforce the provisions of this*
465   *chapter, subject to appropriation.*
466   **2. The Chairman of the Joint Commission on Technology and Science shall create a work group**
467   **composed of the Secretary of Commerce and Trade, the Secretary of Administration, the Attorney**
468   **General, the Chairman of the Senate Committee on Transportation, representatives of businesses**
469   **who control or process personal data of at least 100,000 persons, and consumer rights advocates.**
470   **The work group shall review the provisions of this act and issues related to its implementation.**
471   **The Chairman of the Joint Commission on Technology and Science shall submit the work group's**
472   **findings, best practices, and recommendations regarding the implementation of this act to the**
473   **Chairmen of the Senate Committee on General Laws and Technology and the House Committee**
474   **on Communications, Technology and Innovation no later than November 1, 2021.**
475   **3. That any reference to federal law or statute in this act shall be deemed to include any**
476   **accompanying rules or regulations or exemptions thereto. Further, this enactment is declaratory of**
477   **existing law.**
478   **4. That the provisions of the first and third enactments of this act shall become effective on**
479   **January 1, 2023.**