

1 VIRGINIA ACTS OF ASSEMBLY — CHAPTER

2 *An Act to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 58, consisting of sections*
 3 *numbered 59.1-607 through 59.1-612, relating to high-risk artificial intelligence; development,*
 4 *deployment, and use; civil penalties.*

5 [H 2094]

6 Approved

7 **Be it enacted by the General Assembly of Virginia:**

8 **1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 58, consisting of**
 9 **sections numbered 59.1-607 through 59.1-612, as follows:**

10 CHAPTER 58.

11 HIGH-RISK ARTIFICIAL INTELLIGENCE DEVELOPER AND DEPLOYER ACT.

12 § 59.1-607. *Definitions.*13 *As used in this chapter, unless the context requires a different meaning:*

14 *"Algorithmic discrimination" means the use of an artificial intelligence system that results in an unlawful*
 15 *differential treatment or impact that disfavors an individual or group of individuals on the basis of their*
 16 *actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English*
 17 *language, national origin, race, religion, reproductive health, sex, sexual orientation, veteran status, or other*
 18 *classification protected under state or federal law. "Algorithmic discrimination" does not include (i) the*
 19 *offer, license, or use of a high-risk artificial intelligence system by a developer or deployer for the sole*
 20 *purpose of the developer's or deployer's self-testing to identify, mitigate, or prevent discrimination or*
 21 *otherwise ensure compliance with state and federal law; (ii) the expansion of an applicant, customer, or*
 22 *participant pool to increase diversity or redress historical discrimination; or (iii) an act or omission by or on*
 23 *behalf of a private club or other establishment not in fact open to the public, as set forth in Title II of the Civil*
 24 *Rights Act of 1964, 42 U.S.C. § 2000a(e), as amended from time to time.*

25 *"Artificial intelligence system" means any machine learning-based system that, for any explicit or implicit*
 26 *objective, infers from the inputs such system receives how to generate outputs, including content, decisions,*
 27 *predictions, and recommendations, that can influence physical or virtual environments. "Artificial*
 28 *intelligence system" does not include any artificial intelligence system or general purpose artificial*
 29 *intelligence model that is used for development, prototyping, and research activities before such artificial*
 30 *intelligence system or general purpose artificial intelligence model is made available to deployers or*
 31 *consumers.*

32 *"Consequential decision" means any decision that has a material legal, or similarly significant, effect on*
 33 *the provision or denial to any consumer of (i) parole, probation, a pardon, or any other release from*
 34 *incarceration or court supervision; (ii) education enrollment or an education opportunity; (iii) access to*
 35 *employment; (iv) a financial or lending service; (v) access to health care services; (vi) housing; (vii)*
 36 *insurance; (viii) marital status; or (ix) a legal service.*

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

40 *"Deployer" means any person doing business in the Commonwealth that deploys or uses a high-risk*
 41 *artificial intelligence system to make a consequential decision in the Commonwealth.*

42 *"Developer" means any person doing business in the Commonwealth that develops or intentionally and*
 43 *substantially modifies a high-risk artificial intelligence system that is offered, sold, leased, given, or*
 44 *otherwise made available to deployers or consumers in the Commonwealth.*

45 *"Facial recognition" means the use of a computer system that, for the purpose of attempting to determine*
 46 *the identity of an unknown individual, uses an algorithm to compare the facial biometric data of an unknown*
 47 *individual derived from a photograph, video, or image to a database of photographs or images and*
 48 *associated facial biometric data in order to identify potential matches to an individual. "Facial recognition"*
 49 *does not include facial verification technology, which involves the process of comparing an image or facial*
 50 *biometric data of a known individual, where such information is provided by that individual, to an image*
 51 *database, or to government documentation containing an image of the known individual, to identify a*
 52 *potential match in pursuit of the individual's identity.*

53 *"General-purpose artificial intelligence model" means a model used by an artificial intelligence system or*
 54 *other system that (i) displays significant generality, (ii) is capable of competently performing a wide range of*
 55 *distinct tasks, and (iii) can be integrated into a variety of downstream applications or systems. "General-*
 56 *purpose artificial intelligence model" does not include any artificial intelligence model that is used for*

57 development, prototyping, and research activities before such artificial intelligence model is made available
58 to deployers or consumers.

59 "Generative artificial intelligence" means an artificial intelligence system that is capable of producing
60 and used to produce synthetic content, including audio, images, text, and videos.

61 "Generative artificial intelligence system" means any artificial intelligence system or service that
62 incorporates generative artificial intelligence.

63 "High-risk artificial intelligence system" means any artificial intelligence system that is specifically
64 intended to autonomously make, or be a substantial factor in making, a consequential decision. A system or
65 service is not a "high-risk artificial intelligence system" if it is intended to (i) perform a narrow procedural
66 task, (ii) improve the result of a previously completed human activity, (iii) detect any decision-making
67 patterns or any deviations from pre-existing decision-making patterns, or (iv) perform a preparatory task to
68 an assessment relevant to a consequential decision. "High-risk artificial intelligence system" does not include
69 any of the following technologies:

70 1. Anti-fraud technology that does not use facial recognition technology;

71 2. Anti-malware technology;

72 3. Anti-virus technology;

73 4. Artificial intelligence-enabled video games;

74 5. Autonomous vehicle technology;

75 6. Calculators;

76 7. Cybersecurity technology;

77 8. Databases;

78 9. Data storage;

79 10. Firewall technology;

80 11. Internet domain registration;

81 12. Internet website loading;

82 13. Networking;

83 14. Spam and robocall filtering;

84 15. Spell-checking technology;

85 16. Spreadsheets;

86 17. Web caching;

87 18. Web hosting or any similar technology; or

88 19. Technology that communicates with consumers in natural language for the purpose of providing users
89 with information, making referrals or recommendations, and answering questions and is subject to an
90 acceptable use policy that prohibits generating content that is discriminatory or unlawful.

91 "Intentional and substantial modification" means any deliberate change made to (i) an artificial
92 intelligence system that results, at the time when the change is implemented and any time thereafter, in any
93 new material risk of algorithmic discrimination or (ii) a general-purpose artificial intelligence model that
94 affects compliance of the general-purpose artificial intelligence model, materially changes the purpose of the
95 general-purpose artificial intelligence model, or results in any new reasonably foreseeable risk of
96 algorithmic discrimination. "Intentional and substantial modification" does not include (a) any customization
97 made by deployers that (1) is based on legitimate nondiscriminatory business justifications, (2) is within the
98 scope and purpose of the artificial intelligence tool, and (3) that does not result in a material change to the
99 risks of algorithmic discrimination or (b) any change made to a high-risk artificial intelligence system, or the
100 performance of a high-risk artificial intelligence system, if (1) the high-risk artificial intelligence system
101 continues to learn after such high-risk artificial intelligence system is offered, sold, leased, licensed, given, or
102 otherwise made available to a deployer, or deployed, and (2) such change (A) is made to such high-risk
103 artificial intelligence system as a result of any learning described in clause (b) (1) and (B) was
104 predetermined by the deployer or the third party contracted by the deployer and included within the initial
105 impact assessment of such high-risk artificial intelligence system as required in § 59.1-609.

106 "Machine learning" means the development of algorithms to build data-derived statistical models that are
107 capable of drawing inferences from previously unseen data without explicit human instruction.

108 "Person" includes any individual, corporation, partnership, association, cooperative, limited liability
109 company, trust, joint venture, or any other legal or commercial entity and any successor, representative,
110 agent, agency, or instrumentality thereof. "Person" does not include any government or political subdivision.

111 "Principal basis" means the use of an output of a high-risk artificial intelligence system to make a
112 decision without (i) human review, oversight, involvement, or intervention or (ii) meaningful consideration by
113 a human.

114 "Red-teaming" means adversarial testing to identify the potential adverse behaviors or outcomes of an
115 artificial intelligence system, identify how such behaviors or outcomes occur, and stress test the safeguards
116 against such behaviors or outcomes.

117 "Substantial factor" means a factor that (i) uses the principal basis for making a consequential decision,
118 (ii) is capable of altering the outcome of a consequential decision, and (iii) is generated by an artificial

119 intelligence system. "Substantial factor" includes any use of an artificial intelligence system to generate any
 120 content, decision, prediction, or recommendation concerning a consumer that is used as the principal basis
 121 to make a consequential decision concerning the consumer.

122 "Synthetic content" means information, such as images, video, audio clips, and, to the extent practicable,
 123 text, that has been significantly modified or generated by algorithms, including by artificial intelligence.

124 "Trade secret" means information, including a formula, pattern, compilation, program, device, method,
 125 technique, or process, that (i) derives independent economic value, actual or potential, from not being
 126 generally known to, and not being readily ascertainable by proper means by, other persons who can obtain
 127 economic value from its disclosure or use and (ii) is the subject of efforts that are reasonable under the
 128 circumstances to maintain its secrecy.

129 **§ 59.1-608. Operating standards for developers of high-risk artificial intelligence systems.**

130 A. Each developer of a high-risk artificial intelligence system shall use a reasonable duty of care to
 131 protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising
 132 from the intended and contracted uses. In any enforcement action brought by the Attorney General pursuant
 133 to § 59.1-611, there shall be a rebuttable presumption that a developer of a high-risk artificial intelligence
 134 system used a reasonable duty of care as required by this subsection if the developer complied with the
 135 requirements of this section.

136 B. No developer of a high-risk artificial intelligence system shall offer, sell, lease, give, or otherwise
 137 provide to a deployer or other developer a high-risk artificial intelligence system unless the developer makes
 138 available to the deployer or other developer:

139 1. A statement disclosing the intended uses of such high-risk artificial intelligence system;

140 2. Documentation disclosing the following:

141 a. The known or reasonably known limitations of such high-risk artificial intelligence system, including
 142 any and all known or reasonably foreseeable risks of algorithmic discrimination arising from the intended
 143 uses of such high-risk artificial intelligence system;

144 b. The purpose of such high-risk artificial intelligence system and the intended benefits and uses of such
 145 high-risk artificial intelligence system;

146 c. A summary describing how such high-risk artificial intelligence system was evaluated for performance
 147 before such high-risk artificial intelligence system was licensed, sold, leased, given, or otherwise made
 148 available to a deployer or other developer;

149 d. The measures the developer has taken to mitigate reasonable foreseeable risks of algorithmic
 150 discrimination that the developer knows arises from deployment or use of such high-risk artificial
 151 intelligence system; and

152 e. How an individual can use such high-risk artificial intelligence system and monitor the performance of
 153 such high-risk artificial intelligence system for any risk of algorithmic discrimination;

154 3. Documentation including (i) a description of how the high-risk artificial intelligence system was
 155 evaluated for performance and for mitigation of algorithmic discrimination before such system was made
 156 available to the deployer or other developer; (ii) a description of the intended outputs of the high-risk
 157 artificial intelligence system; (iii) a description of the measures the developer has taken to mitigate known or
 158 reasonably foreseeable risks of algorithmic discrimination that may arise from the reasonably foreseeable
 159 deployment of the high-risk artificial intelligence system; and (iv) a description of how the high-risk artificial
 160 intelligence system should be used, not be used, and be monitored by an individual when such system is used
 161 to make, or is a substantial factor in making, a consequential decision; and

162 4. Any additional documentation that is reasonably necessary to assist the deployer or other developer in
 163 understanding the outputs and monitoring performance of the high-risk artificial intelligence system for risks
 164 of algorithmic discrimination.

165 C. Each developer that offers, sells, leases, gives, or otherwise makes available to a deployer or other
 166 developer a high-risk artificial intelligence system shall make available to the deployer or other developer to
 167 the extent feasible and necessary, information and documentation through artifacts such as system cards or
 168 predeployment impact assessments, including any risk management policy designed and implemented and
 169 any relevant impact assessment completed, and such documentation and information shall enable the
 170 deployer, other developer, or a third party contracted by the deployer to complete an impact assessment as
 171 required in § 59.1-609.

172 D. A developer that also serves as a deployer for any high-risk artificial intelligence system shall not be
 173 required to generate the documentation required by this section unless such high-risk artificial intelligence
 174 system is provided to an unaffiliated entity acting as a deployer or as otherwise required by law.

175 E. Nothing in this section shall be construed to require a developer to disclose any trade secret,
 176 information that could create a security risk, or other confidential or proprietary information protected under
 177 state or federal law.

178 F. High-risk artificial intelligence systems that are in conformity with the latest version of the Artificial
 179 Intelligence Risk Management Framework published by the National Institute of Standards and Technology,
 180 Standard ISO/IEC 42001 of the International Organization for Standardization, or another nationally or

181 internationally recognized risk management framework for artificial intelligence systems, or parts thereof,
182 shall be presumed to be in conformity with related requirements set out in this section and in associated
183 regulations.

184 G. For any disclosure required pursuant to this section, each developer shall, no later than 90 days after
185 the developer performs an intentional and substantial modification to any high-risk artificial intelligence
186 system, update such disclosure as necessary to ensure that such disclosure remains accurate.

187 H. 1. Each developer of a high-risk generative artificial intelligence system that generates or substantially
188 modifies synthetic content shall ensure that the outputs of such high-risk artificial intelligence system (i) are
189 identifiable and detectable in a manner that is accessible by consumers using industry-standard tools or tools
190 provided by the developer; (ii) comply with any applicable accessibility requirements, as synthetic content, to
191 the extent reasonably feasible; and (iii) apply such identification at the time the output is generated;

192 2. If such synthetic content is an audio, image, or video format that forms part of an evidently artistic,
193 creative, satirical, fictional analogous work or program, such requirement for identifying outputs of high-risk
194 artificial intelligence systems pursuant to subdivision 1 shall be limited to a manner that does not hinder the
195 display or enjoyment of such work or program.

196 3. The identification of outputs required by subdivision 1 shall not apply to (i) synthetic content that
197 consists exclusively of text, is published to inform the public on any matter of public interest, or is unlikely to
198 mislead a reasonable person consuming such synthetic content or (ii) the outputs of a high-risk artificial
199 intelligence system that performs an assistive function for standard editing, does not substantially alter the
200 input data provided by the developer, or is used to detect, prevent, investigate, or prosecute any crime as
201 authorized by law.

202 I. Where multiple developers directly contribute to the development of a high-risk artificial intelligence
203 system, each developer shall be subject to the obligations and operating standards applicable to developers
204 pursuant to this section solely with respect to its activities contributing to the development of the high-risk
205 artificial intelligence system.

206 **§ 59.1-609. Operating standards for deployers of high-risk artificial intelligence systems.**

207 A. Each deployer of a high-risk artificial intelligence system shall use a reasonable duty of care to protect
208 consumers from any known or reasonably foreseeable risks of algorithmic discrimination. In any
209 enforcement action brought by the Attorney General pursuant to § 59.1-611, there shall be a rebuttable
210 presumption that a deployer of a high-risk artificial intelligence system used a reasonable duty of care as
211 required by this subsection if the deployer complied with the provisions of this section.

212 B. No deployer shall deploy or use a high-risk artificial intelligence system to make a consequential
213 decision unless the deployer has designed and implemented a risk management policy and program for such
214 high-risk artificial intelligence system. The risk management policy shall specify the principles, processes,
215 and personnel that the deployer shall use in maintaining the risk management program to identify, mitigate,
216 and document any risk of algorithmic discrimination that is a reasonably foreseeable consequence of
217 deploying or using such high-risk artificial intelligence system to make a consequential decision. Each risk
218 management policy and program designed, implemented, and maintained pursuant to this subsection shall be
219 reasonable considering the guidance and standards set forth in the latest version of:

220 1. The Artificial Intelligence Risk Management Framework published by the National Institute of
221 Standards and Technology;

222 2. Standard ISO/IEC 42001 of the International Organization for Standardization;

223 3. A nationally or internationally recognized risk management framework for artificial intelligence
224 systems with requirements that are substantially equivalent to, and at least as stringent as, the requirements
225 set forth in this section; or

226 4. Any risk management framework for artificial intelligence systems that the Attorney General may
227 designate and is substantially equivalent to, and at least as stringent as, the guidance and standards
228 described in subdivision 1.

229 High-risk artificial intelligence systems that are in conformity with the latest version of the Artificial
230 Intelligence Risk Management Framework published by the National Institute of Standards and Technology,
231 Standard ISO/IEC 42001 of the International Organization for Standardization, or another nationally or
232 internationally recognized risk management framework for artificial intelligence systems, or parts thereof,
233 shall be presumed to be in conformity with related requirements set out in this section and in associated
234 regulations.

235 C. Except as provided in this subsection, no deployer shall deploy or use a high-risk artificial intelligence
236 system to make a consequential decision unless the deployer has completed an impact assessment for such
237 high-risk artificial intelligence system. The deployer shall complete an impact assessment for a high-risk
238 artificial intelligence system (i) before the deployer initially deploys such high-risk artificial intelligence
239 system and (ii) before a significant update to such high-risk artificial intelligence system is used to make a
240 consequential decision.

241 Each impact assessment completed pursuant to this subsection shall include, at a minimum:

242 1. A statement by the deployer disclosing (i) the purpose, intended use cases and deployment context of,

243 and benefits afforded by the high-risk artificial intelligence system and (ii) whether the deployment or use of
 244 the high-risk artificial intelligence system poses any known or reasonably foreseeable risk of algorithmic
 245 discrimination and, if so, (a) the nature of such algorithmic discrimination and (b) the steps that have been
 246 taken, to the extent feasible, to mitigate such risk;

247 2. For each post-deployment impact assessment completed pursuant to this subsection, whether the
 248 intended use cases of the high-risk artificial intelligence system as updated were consistent with, or varied
 249 from, the developer's intended uses of such high-risk artificial intelligence system;

250 3. A description of (i) the categories of data the high-risk artificial intelligence system processes as inputs
 251 and (ii) the outputs such high-risk artificial intelligence system produces;

252 4. If the deployer used data to customize the high-risk artificial intelligence system, an overview of the
 253 categories of data the deployer used to customize such high-risk artificial intelligence system;

254 5. A list of any metrics used to evaluate the performance and known limitations of the high-risk artificial
 255 intelligence system;

256 6. A description of any transparency measures taken concerning the high-risk artificial intelligence
 257 system, including any measures taken to disclose to a consumer that such high-risk artificial intelligence
 258 system is in use when such high-risk artificial intelligence system is in use;

259 7. A description of any post-deployment monitoring performed and user safeguards provided concerning
 260 such high-risk artificial intelligence system, including any oversight process established by the deployer to
 261 address issues arising from deployment or use of such high-risk artificial intelligence system as such issues
 262 arise; and

263 8. An analysis of such high-risk artificial intelligence system's validity and reliability in accordance with
 264 standard industry practices and a description of any metrics used to evaluate the performance and known
 265 limitations of such high-risk artificial intelligence system.

266 A single impact assessment may address a comparable set of high-risk artificial intelligence systems
 267 deployed or used by a deployer. High-risk artificial intelligence systems that are in conformity with the latest
 268 version of the Artificial Intelligence Risk Management Framework published by the National Institute of
 269 Standards and Technology, Standard ISO/IEC 42001 of the International Organization for Standardization,
 270 or another nationally or internationally recognized risk management framework for artificial intelligence
 271 systems, or parts thereof, shall be presumed to be in conformity with related requirements set out in this
 272 section and in associated regulations. If a deployer completes an impact assessment for the purpose of
 273 complying with another applicable law or regulation, such impact assessment shall be deemed to satisfy the
 274 requirements established in this subsection if such impact assessment is reasonably similar in scope and
 275 effect to the impact assessment that would otherwise be completed pursuant to this subsection. A deployer
 276 that completes an impact assessment pursuant to this subsection shall maintain such impact assessment and
 277 all records concerning such impact assessment for three years.

278 Throughout the period of time that a high-risk artificial intelligence system is deployed and for a period of
 279 at least three years following the final deployment of such high-risk artificial intelligence system, the
 280 deployer shall retain all records concerning each impact assessment conducted on the high-risk artificial
 281 intelligence system, including all raw data used to evaluate the performance and known limitations of such
 282 system.

283 D. Not later than the time that a deployer uses a high-risk artificial intelligence system to interact with a
 284 consumer, the deployer shall disclose to the consumer that the deployer is interacting with an artificial
 285 intelligence system disclosing (i) the purpose of such high-risk artificial intelligence system, (ii) the nature of
 286 such system, (iii) the nature of the consequential decision, (iv) the contact information for the deployer, and
 287 (v) a description of the artificial intelligence system in plain language of such system, which shall include (a)
 288 a description of the personal characteristics or attributes that such system will measure or assess, (b) the
 289 method by which the system measures or assesses such attributes or characteristics, (c) how such attributes
 290 or characteristics are relevant to the consequential decisions for which the system should be used, (d) any
 291 human components of such system, and (e) how any automated components of such system are used to inform
 292 such consequential decisions.

293 A deployer that has deployed a high-risk artificial intelligence system to make a consequential decision
 294 concerning a consumer shall transmit to the consumer the consequential decision without undue delay. If
 295 such consequential decision is adverse to such consumer and based on personal data beyond information that
 296 the consumer provided directly to the deployer, the deployer shall provide to the consumer (a) a statement
 297 disclosing the principal reason or reasons for the consequential decision, including (1) the degree to which
 298 and manner in which the high-risk artificial intelligence system contributed to the consequential decision, (2)
 299 the type of data that was processed by such system in making the consequential decision, and (3) the sources
 300 of such data; (b) pursuant to the provisions of the Consumer Data Protection Act (§ 59.1-575 et seq.), an
 301 opportunity to correct any inaccuracies in the consumer's personal data that the high-risk artificial
 302 intelligence system processed in making, or as a substantial factor in making, the consequential decision; and
 303 (c) an opportunity to appeal such adverse consequential decision concerning the consumer arising from the
 304 deployment of such system. Any such appeal shall allow for human review, if technically reasonable and

305 *practicable, unless providing the opportunity for appeal is not in the best interest of the consumer, including*
306 *instances in which any delay might pose a risk to the life or safety of such consumer.*

307 *E. Each deployer shall make available, in a manner that is clear and readily available, a statement*
308 *summarizing how such deployer manages any reasonably foreseeable risk of algorithmic discrimination that*
309 *may arise from the use or deployment of the high-risk artificial intelligence system.*

310 *F. For any disclosure required pursuant to this section, each deployer shall, no later than 30 days after*
311 *the deployer is notified by the developer that the developer has performed an intentional and substantial*
312 *modification to any high-risk artificial intelligence system, update such disclosure as necessary to ensure that*
313 *such disclosure remains accurate.*

314 *G. Any deployer who performs an intentional and substantial modification to any high-risk artificial*
315 *intelligence system shall comply with the documentation and disclosure requirements for developers pursuant*
316 *to subsections B through G of § 59.1-608.*

317 *H. Nothing in this section shall be construed to require a deployer to disclose any trade secret,*
318 *information that could create a security risk, or other confidential or proprietary information protected under*
319 *state or federal law.*

320 **§ 59.1-610. Exemptions.**

321 *A. Nothing in this chapter shall be construed to restrict a developer's or deployer's ability to (i) comply*
322 *with federal, state, or municipal ordinances or regulations; (ii) comply with a civil, criminal, or regulatory*
323 *inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; (iii)*
324 *cooperate with law-enforcement agencies concerning conduct or activity that the developer or deployer*
325 *reasonably and in good faith believes may violate federal, state, or local law, ordinances, or regulations; (iv)*
326 *investigate, establish, exercise, prepare for, or defend legal claims; (v) provide a product or service*
327 *specifically requested by a consumer; (vi) perform under a contract to which a consumer is a party, including*
328 *fulfilling the terms of a written warranty; (vii) take steps at the request of a consumer prior to entering into a*
329 *contract; (viii) take immediate steps to protect an interest that is essential for the life or physical safety of the*
330 *consumer or another individual; (ix) prevent, detect, protect against, or respond to security incidents, identity*
331 *theft, fraud, harassment, or malicious or deceptive activities; (x) take actions to prevent, detect, protect*
332 *against, report, or respond to the production, generation, incorporation, or synthesization of child sex abuse*
333 *material, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or*
334 *prosecute those responsible for any such action; (xi) engage in public or peer-reviewed scientific or*
335 *statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is*
336 *approved, monitored, and governed by an institutional review board that determines, or similar independent*
337 *oversight entities that determine, (a) that the expected benefits of the research outweigh the risks associated*
338 *with such research and (b) whether the developer or deployer has implemented reasonable safeguards to*
339 *mitigate the risks associated with such research; (xii) assist another developer or deployer with any of the*
340 *obligations imposed by this chapter; or (xiii) take any action that is in the public interest in the areas of*
341 *public health, community health, or population health, but solely to the extent that such action is subject to*
342 *suitable and specific measures to safeguard the public.*

343 *B. The obligations imposed on developers or deployers by this chapter shall not restrict a developer's or*
344 *deployer's ability to (i) conduct internal research to develop, improve, or repair products, services, or*
345 *technologies; (ii) effectuate a product recall; (iii) identify and repair technical errors that impair existing or*
346 *intended functionality; or (iv) perform internal operations that are reasonably aligned with the expectations*
347 *of the consumer or reasonably anticipated based on the consumer's existing relationship with the developer*
348 *or deployer.*

349 *C. Nothing in this chapter shall be construed to impose any obligation on a developer or deployer to*
350 *disclose trade secrets or information protected from disclosure by state or federal law.*

351 *D. The obligations imposed on developers or deployers by this chapter shall not apply where compliance*
352 *by the developer or deployer with such obligations would violate an evidentiary privilege under federal law*
353 *or the laws of the Commonwealth.*

354 *E. Nothing in this chapter shall be construed to impose any obligation on a developer or deployer that*
355 *adversely affects the legally protected rights or freedoms of any person, including the rights of any person to*
356 *freedom of speech or freedom of the press guaranteed in the First Amendment to the Constitution of the*
357 *United States or under the Virginia Human Rights Act (§ 2.2-3900 et seq.).*

358 *F. The obligations imposed on developers or deployers by this chapter shall not apply to any artificial*
359 *intelligence system that is acquired by or for the federal government or any federal agency or department,*
360 *including the U.S. Department of Commerce, the U.S. Department of Defense, and the National Aeronautics*
361 *and Space Administration, unless such artificial intelligence system is a high-risk artificial intelligence*
362 *system that is used to make, or is a substantial factor in making, a decision concerning employment or*
363 *housing.*

364 *G. For the purposes of this subsection:*

365 *"Affiliate" means the same as that term is defined in § 6.2-899.*

366 *"Bank" means the same as that term is defined in § 6.2-800.*

367 "Credit union" means the same as that term is defined in § 6.2-1300.

368 "Federal credit union" means a credit union duly organized under federal law.

369 "Mortgage lender" means the same as that term is defined in § 6.2-1600.

370 "Out-of-state bank" means the same as that term is defined in § 6.2-836.

371 "Out-of-state credit union" means a credit union organized and doing business in another state.

372 "Savings institution" means the same as that term is defined in § 6.2-1100.

373 "Subsidiary" means the same as that term is defined in § 6.2-700.

374 The obligations imposed on developers or deployers by this chapter shall be deemed satisfied for any
375 bank, out-of-state bank, credit union, federal credit union, mortgage lender, out-of-state credit union, savings
376 institution, or any affiliate, subsidiary, or service provider thereof if such bank, out-of-state bank, credit
377 union, federal credit union, mortgage lender, out-of-state credit union, savings institution, or affiliate,
378 subsidiary, or service provider is subject to the jurisdiction of any state or federal regulator under any
379 published guidance or regulations that apply to the use of high-risk artificial intelligence systems and such
380 guidance or regulations.

381 H. For purposes of this subsection, "insurer" means the same as that term is defined in § 38.2-100.

382 The provisions of this chapter shall not apply to any insurer, or any high-risk artificial intelligence system
383 developed by or for or deployed by an insurer for use in the business of insurance, if such insurer is regulated
384 and supervised by the State Corporation Commission or a comparable federal regulating body and subject to
385 examination by such entity under any existing statutes, rules, or regulations pertaining to unfair trade
386 practices and unfair discrimination prohibited under Chapter 5 (§ 38.2-500 et seq.) of Title 38.2, or
387 published guidance or regulations that apply to the use of high-risk artificial intelligence systems and such
388 guidance or regulations aid in the prevention and mitigation of algorithmic discrimination caused by the use
389 of a high-risk artificial intelligence system or any risk of algorithmic discrimination that is reasonably
390 foreseeable as a result of the use of a high-risk artificial intelligence system. Nothing in this chapter shall be
391 construed to delegate existing regulatory oversight of the business of insurance to any department or agency
392 other than the Bureau of Insurance of the Virginia State Corporation Commission.

393 I. The provisions of this chapter shall not apply to the development of an artificial intelligence system that
394 is used exclusively for research, training, testing, or other pre-deployment activities performed by active
395 participants of any sandbox software or sandbox environment established and subject to oversight by a
396 designated agency or other government entity and that is in compliance with the provisions of this chapter.

397 J. The provisions of this chapter shall not apply to a developer or deployer, or other person who develops,
398 deploys, puts into service, or intentionally modifies, as applicable, a high-risk artificial intelligence system
399 that (i) has been approved, authorized, certified, cleared, developed, or granted by a federal agency acting
400 within the scope of the federal agency's authority, or by a regulated entity subject to the supervision and
401 regulation of the Federal Housing Finance Agency or (ii) is in compliance with standards established by a
402 federal agency or by a regulated entity subject to the supervision and regulation of the Federal Housing
403 Finance Agency, if the standards are substantially equivalent or more stringent than the requirements of this
404 chapter.

405 K. The provisions of this chapter shall not apply to a developer or deployer, or other person that (i)
406 facilitates or engages in the provision of telehealth services, as defined in § 32.1-122.03:1, or (ii) is a
407 covered entity within the meaning of the federal Health Insurance Portability and Accountability Act of 1996
408 (42 U.S.C. § 1320d et seq.) and the regulations promulgated under such federal act, as both may be amended
409 from time to time, and is providing (a) health care recommendations that (1) are generated by an artificial
410 intelligence system and (2) require a health care provider, as defined in § 8.01-581.1, to take action to
411 implement the recommendations or (b) services utilizing an artificial intelligence system for an
412 administrative, quality measurement, security, or internal cost or performance improvement function.

413 L. If a developer or deployer engages in any action authorized by an exemption set forth in this section,
414 the developer or deployer bears the burden of demonstrating that such action qualifies for such exemption.

415 M. If a developer or deployer withholds information pursuant to an exemption set forth in this chapter for
416 which disclosure would otherwise be required by this chapter, including the exemption from disclosure of
417 trade secrets, the developer or deployer shall notify the subject of disclosure and provide a basis for
418 withholding the information. If a developer or deployer redacts any information pursuant to an exemption
419 from disclosure, the developer or deployer shall notify the subject of disclosure that the developer or
420 deployer is redacting such information and provide the basis for such decision to redact.

421 **§ 59.1-611. Enforcement; civil penalties.**

422 A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

423 B. Whenever the Attorney General has reasonable cause to believe that any person has engaged in or is
424 engaging in any violation of this chapter, the Attorney General is empowered to issue a civil investigative
425 demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued
426 pursuant to this section. In rendering and furnishing any information requested pursuant to a civil
427 investigative demand issued pursuant to this section, a developer or deployer may redact or omit any trade
428 secrets or information protected from disclosure by state or federal law. If a developer or deployer refuses to

429 disclose, redacts, or omits information based on the exemption from disclosure of trade secrets, such
430 developer or deployer shall affirmatively state to the Attorney General that the basis for nondisclosure,
431 redaction, or omission is because such information is a trade secret. To the extent that any information
432 requested pursuant to a civil investigative demand issued pursuant to this section is subject to attorney-client
433 privilege or work-product protection, disclosure of such information pursuant to the civil investigative
434 demand shall not constitute a waiver of such privilege or protection. Any information, statement, or
435 documentation provided to the Attorney General pursuant to this section shall be exempt from disclosure
436 under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).

437 C. Notwithstanding any contrary provision of law, the Attorney General may cause an action to be
438 brought in the appropriate circuit court in the name of the Commonwealth to enjoin any violation of this
439 chapter. The circuit court having jurisdiction may enjoin such violation notwithstanding the existence of an
440 adequate alternative remedy at law.

441 D. Any person who violates the provisions of this chapter shall be subject to a civil penalty in an amount
442 not to exceed \$1,000 plus reasonable attorney fees, expenses, and costs, as determined by the court. Any
443 person who willfully violates the provisions of this chapter shall be subject to a civil penalty in an amount not
444 less than \$1,000 and not more than \$10,000 plus reasonable attorney fees, expenses, and costs, as
445 determined by the court. Such civil penalties shall be paid into the Literary Fund.

446 E. Each violation of this chapter shall constitute a separate violation and shall be subject to any civil
447 penalties imposed under this section.

448 F. The Attorney General may require that a developer disclose to the Attorney General any statement or
449 documentation described in this chapter if such statement or documentation is relevant to an investigation
450 conducted by the Attorney General. The Attorney General may also require that a deployer disclose to the
451 Attorney General any risk management policy designed and implemented, impact assessment completed, or
452 record maintained pursuant to this chapter if such risk management policy, impact assessment, or record is
453 relevant to an investigation conducted by the Attorney General.

454 G. In an action brought by the Attorney General pursuant to this section, it shall be an affirmative defense
455 that the developer or deployer (i) discovers a violation of any provision of this chapter through red-teaming
456 or other method; (ii) no later than 45 days after discovering such violation (a) cures such violation and (b)
457 provides notice to the Attorney General in a form and manner as prescribed by the Attorney General that
458 such violation has been cured and evidence that any harm caused by such violation has been mitigated; and
459 (iii) is otherwise in compliance with the requirements of this chapter.

460 H. Prior to causing an action against a developer or deployer for a violation of this chapter pursuant to
461 subsection C, the Attorney General shall determine, in consultation with the developer or deployer, if it is
462 possible to cure the violation. If it is possible to cure such violation, the Attorney General may issue a notice
463 of violation to the developer or deployer and afford the developer or deployer the opportunity to cure such
464 violation within 45 days of the receipt of such notice of violation. In determining whether to grant such
465 opportunity to cure such violation, the Attorney General shall consider (i) the number of violations; (ii) the
466 size and complexity of the developer or deployer; (iii) the nature and extent of the developer's or deployer's
467 business; (iv) the substantial likelihood of injury to the public; (v) the safety of persons or property; and (vi)
468 whether such violation was likely caused by human or technical error. If the developer or deployer fails to
469 cure such violation within 45 days of the receipt of such notice of violation, the Attorney General may
470 proceed with such action.

471 I. Nothing in this chapter shall create a private cause of action in favor of any person aggrieved by a
472 violation of this chapter.

473 **§ 59.1-612. Construction of chapter.**

474 A. This chapter is declared to be remedial, with the purposes of protecting consumers and ensuring
475 consumers receive information about consequential decisions affecting them. The provisions of this chapter
476 granting rights or protections to consumers shall be construed broadly and exemptions construed narrowly.

477 B. If any provision of this chapter or its application to any person or circumstance is held invalid, the
478 invalidity shall not affect other provisions or applications of this chapter that can be given effect without the
479 invalid provision or application, and to this end all the provisions of this chapter are hereby expressly
480 declared to be severable.

481 **2. That the provisions of this act shall become effective on July 1, 2026.**

482 **3. That compliance with the provisions of Chapter 58 (§ 59.1-607 et seq.) of Title 59.1 of the Code of**
483 **Virginia, as created by this act, shall not (i) relieve a person from liability for any causes of action that**
484 **existed at common law or by statute prior to July 1, 2026, or (ii) be construed to modify or otherwise**
485 **affect, preempt, limit, or displace any causes of action that existed at common law or by statute prior to**
486 **July 1, 2026.**