

24105096D

**HOUSE BILL NO. 747**

Offered January 10, 2024

Prefiled January 9, 2024

A *BILL to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 57, consisting of sections numbered 59.1-603 through 59.1-608, relating to Artificial Intelligence Developer Act established; civil penalty.*

Patron—Maldonado

Referred to Committee on Communications, Technology and Innovation

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

**1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 57, consisting of sections numbered 59.1-603 through 59.1-608, as follows:**

**CHAPTER 57.**

**ARTIFICIAL INTELLIGENCE DEVELOPER ACT.**

**§ 59.1-603. Definitions.**

*As used in this chapter, unless the context requires a different meaning:*

*"Algorithmic discrimination" means any discrimination that is (i) prohibited under state or federal law and (ii) a reasonably foreseeable consequence of deploying or using a high-risk artificial intelligence system to make a consequential decision.*

*"Artificial intelligence" means technology that uses data to train statistical models for the purpose of enabling a computer system or service to autonomously perform any task, including visual perception, language processing, and speech recognition, that is normally associated with human intelligence or perception.*

*"Artificial intelligence system" means any computer system or service that incorporates artificial intelligence.*

*"Consequential decision" means any decision that has a material legal, or similarly significant, effect on a consumer's access to credit, criminal justice, education, employment, health care, housing, or insurance.*

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

*"Developer" means any person doing business in the Commonwealth that develops or intentionally and substantially modifies (i) a high-risk artificial intelligence system or (ii) a generative artificial intelligence system that is offered, sold, leased, given, or otherwise provided to consumers in the Commonwealth.*

*"Foundation model" means a machine learning model that (i) is trained on broad data at scale, (ii) is designed for generality of output, and (iii) can be adapted to a wide range of distinctive tasks.*

*"Generative artificial intelligence" means any form of artificial intelligence, including a foundation model, that is able to produce synthetic digital content including audio, images, text, and videos.*

*"Generative artificial intelligence system" means any computer system or service that incorporates generative artificial intelligence.*

*"High-risk artificial intelligence system" means any artificial intelligence system that is specifically intended to autonomously make, or be a controlling factor in making, a consequential decision. A system or service is not a "high-risk artificial intelligence system" if it is intended to (i) perform a narrow procedural task, (ii) improve the result of a previously completed human activity, (iii) detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review, or (iv) perform a preparatory task to an assessment relevant to a consequential decision.*

*"Machine learning" means the process by which artificial intelligence is developed using data and algorithms to draw inferences therefrom to automatically adapt or improve its accuracy without explicit programming from a developer.*

*"Search engine" means any computer system or service that (i) searches for and identifies items in a database that correspond to keywords or characters specified by a user and (ii) is offered to or used by any consumer in the Commonwealth.*

*"Search engine operator" means any person that owns or controls a search engine.*

*"Significant update" means any new version, new release, or other update to a high-risk artificial intelligence system that results in significant changes to such high-risk artificial intelligence system's use case, key functionality, or expected outcomes.*

59 "Social media platform" means an electronic medium or service where users may create, share, or  
60 view user-generated content, including videos, photographs, blogs, podcasts, messages, emails, or  
61 website profiles or locations, and create a personal account.

62 "Social media platform operator" means any person that owns or controls a social media platform.

63 "Synthetic digital content" means any digital content, including any audio, image, text, or video, that  
64 is produced by a generative artificial intelligence system.

65 **§ 59.1-604. Operating standards for developers.**

66 A. No developer of a high-risk artificial intelligence system shall offer, sell, lease, give, or otherwise  
67 provide to a deployer a high-risk artificial intelligence system unless the developer provides to the  
68 deployer (i) a statement disclosing the intended uses of such high-risk artificial intelligence system and  
69 (ii) documentation disclosing (a) the known limitations of such high-risk artificial intelligence system,  
70 including any and all reasonably foreseeable risks of algorithmic discrimination arising from the  
71 intended uses of such high-risk artificial intelligence system; (b) the purpose of such high-risk artificial  
72 intelligence system and the intended benefits and uses of such high-risk artificial intelligence system; (c)  
73 a summary describing how such high-risk artificial intelligence system was evaluated for validity and  
74 explainability before such high-risk artificial intelligence system was licensed or sold; (d) the measures  
75 the developer has taken to mitigate any risk of algorithmic discrimination that the developer knows  
76 arises from deployment or use of such high-risk artificial intelligence system; and (e) how an individual  
77 can use such high-risk artificial intelligence system to make, or monitor such high-risk artificial  
78 intelligence system when such high-risk artificial intelligence system is deployed or used to make, a  
79 consequential decision.

80 B. Each developer that offers, sells, leases, gives, or otherwise provides to a deployer a high-risk  
81 artificial intelligence system shall provide to the deployer the technical capability to access, or otherwise  
82 make available to the deployer, all information and documentation in the developer's possession,  
83 custody, or control that the deployer reasonably requires to complete an impact assessment.

84 C. Nothing in this section shall be construed to require a developer to disclose any trade secret.

85 **§ 59.1-605. Operating standards for developers relating to generative artificial intelligence.**

86 A. No developer that develops or intentionally and substantially modifies a generative artificial  
87 intelligence system on or after October 1, 2024, shall offer, sell, lease, give, or otherwise provide such  
88 generative artificial intelligence system to any consumer in the Commonwealth or any person doing  
89 business in the Commonwealth unless such generative artificial intelligence system satisfies the  
90 requirements established in this subsection.

91 Each generative artificial intelligence system described in this section shall (i) reduce and mitigate  
92 the reasonably foreseeable risks described in this section through, for example, the involvement of  
93 independent experts and documentation of any reasonably foreseeable, but non-mitigable, risks; (ii)  
94 exclusively incorporate and process datasets that are subject to data governance measures that are  
95 appropriate for generative artificial intelligence systems, including data governance measures to  
96 examine the suitability of data sources for possible biases and appropriate mitigation; and (iii) achieve,  
97 throughout the life cycle of such generative artificial intelligence system, appropriate levels of  
98 performance, predictability, interpretability, corrigibility, safety, and cybersecurity, as assessed through  
99 appropriate methods, including model evaluation involving independent experts, documented analysis,  
100 and extensive testing, during conceptualization, design, and development of such generative artificial  
101 intelligence system.

102 B. Except as otherwise provided in this subsection, no developer that develops or intentionally and  
103 substantially modifies a generative artificial intelligence system on or after October 1, 2024, shall offer,  
104 sell, lease, give, or otherwise provide such generative artificial intelligence system to any consumer in  
105 the Commonwealth or any person doing business in the Commonwealth unless such developer has  
106 completed an impact assessment for such generative artificial intelligence system pursuant to this  
107 subsection.

108 Each impact assessment completed pursuant to this subsection shall include, at a minimum, an  
109 evaluation of (i) the intended purpose of such generative artificial intelligence system; (ii) the extent to  
110 which such generative artificial intelligence system has been or is likely to be used; (iii) the extent to  
111 which any prior use of such generative artificial intelligence system has harmed the health or safety of  
112 individuals, adversely impacted the fundamental rights of individuals, or given rise to significant  
113 concerns relating to the materialization of such harm or adverse impact, as demonstrated by reports or  
114 documented allegations submitted to authorities of competent jurisdiction; (iv) the potential extent to  
115 which use of such generative artificial intelligence system will harm the health and safety of individuals  
116 or adversely impact the fundamental rights of individuals, including the intensity of such harm or  
117 adverse impact and the number of individuals likely to suffer such harm or adverse impact; (v) the  
118 extent to which individuals who may be harmed or adversely impacted by such generative artificial  
119 intelligence system are dependent on the outcomes produced by such generative artificial intelligence  
120 system because, among other reasons, it is reasonably impossible, for legal or practical reasons, for

such individuals to opt out of such outcomes; (vi) the extent to which individuals who may be harmed or adversely impacted by users of such generative artificial intelligence system are comparatively more vulnerable to such users due, among other factors, to an imbalance of age, economic or social circumstances, knowledge, or power; and (vii) the extent to which the outcomes produced by such generative artificial intelligence system, other than outcomes affecting health and safety, are easily reversible.

A single impact assessment may address a comparable set of generative artificial intelligence systems developed or intentionally and substantially modified by a developer. If a developer completes an impact assessment for the purpose of complying with another applicable law or regulation, such impact assessment shall be deemed to satisfy the requirements established in this subsection if such impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this subsection. A developer that completes an impact assessment pursuant to this subsection shall maintain such impact assessment and all records concerning such impact assessment for a reasonable period of time.

C. Each developer that offers, sells, leases, gives, or otherwise provides any generative artificial intelligence system described in this section to any search engine operator or social media platform operator shall provide to such search engine operator or social media platform operator the technical capability such search engine operator or social media platform operator reasonably requires to perform such search engine operator's or social media platform operator's duties as described in this chapter.

D. Nothing in this section shall be construed to require a developer to disclose any trade secret.

**§ 59.1-606. Operating standards for deployers.**

A. Each deployer shall use reasonable care to avoid any risk of algorithmic discrimination that is a reasonably foreseeable consequence of deploying or using a high-risk artificial intelligence system to make a consequential decision.

B. No deployer shall deploy or use a high-risk artificial intelligence system to make a consequential decision unless the deployer has designed and implemented a risk management policy and program for such high-risk artificial intelligence system. The risk management policy shall specify the principles, processes, and personnel that the deployer shall use in maintaining the risk management program to identify, mitigate, and document any risk of algorithmic discrimination that is a reasonably foreseeable consequence of deploying or using such high-risk artificial intelligence system to make a consequential decision. Each risk management policy and program designed, implemented, and maintained pursuant to this subsection shall be (i) at least as stringent as the latest version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology or another nationally or internationally recognized risk management framework for artificial intelligence systems and (ii) reasonable considering (a) the size and complexity of the deployer; (b) the nature and scope of the high-risk artificial intelligence systems deployed and used by the deployer, including the intended uses of such high-risk artificial intelligence systems; (c) the sensitivity and volume of data processed in connection with the high-risk artificial intelligence systems deployed and used by the deployer; and (d) the cost to the deployer to implement and maintain such risk management program.

C. Except as provided in this subsection, no deployer shall deploy or use a high-risk artificial intelligence system to make a consequential decision unless the deployer has completed an impact assessment for such high-risk artificial intelligence system. The deployer shall complete an impact assessment for a high-risk artificial intelligence system (i) before the deployer initially deploys such high-risk artificial intelligence system and (ii) not later than 90 days after each significant update to such high-risk artificial intelligence system.

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

1. A statement by the deployer disclosing (i) the purpose, intended use cases and deployment context of, and benefits afforded by the high-risk artificial intelligence system and (ii) whether the deployment or use of the high-risk artificial intelligence system poses a reasonably foreseeable risk of algorithmic discrimination and, if so, (a) the nature of such algorithmic discrimination and (b) the steps that have been taken, to the extent feasible, to mitigate such risk;

2. For each post-deployment impact assessment completed pursuant to this section, the extent to which the high-risk artificial intelligence system was used in a manner that was consistent with, or varied from, the developer's intended uses of such high-risk artificial intelligence system;

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

4. If the deployer used data to retrain the high-risk artificial intelligence system, an overview of the type of data the deployer used to retrain such high-risk artificial intelligence system;

5. A description of any transparency measures taken concerning the high-risk artificial intelligence system, including any measures taken to disclose to a consumer in the Commonwealth that such

182 high-risk artificial intelligence system is in use when such high-risk artificial intelligence system is in  
183 use; and

184 6. A description of any post-deployment monitoring performed and user safeguards provided  
185 concerning such high-risk artificial intelligence system, including any oversight process established by  
186 the deployer to address issues arising from deployment or use of such high-risk artificial intelligence  
187 system as such issues arise.

188 A single impact assessment may address a comparable set of high-risk artificial intelligence systems  
189 deployed or used by a deployer. If a deployer completes an impact assessment for the purpose of  
190 complying with another applicable law or regulation, such impact assessment shall be deemed to satisfy  
191 the requirements established in this subsection if such impact assessment is reasonably similar in scope  
192 and effect to the impact assessment that would otherwise be completed pursuant to this subsection. A  
193 deployer that completes an impact assessment pursuant to this subsection shall maintain such impact  
194 assessment and all records concerning such impact assessment for a reasonable period of time.

195 D. Not later than the time that a deployer uses a high-risk artificial intelligence system to make a  
196 consequential decision concerning an individual, the deployer shall notify the individual that the  
197 deployer is using a high-risk artificial intelligence system to make such consequential decision  
198 concerning such individual and provide to the individual a statement disclosing the purpose of such  
199 high-risk artificial intelligence system.

200 E. Each deployer shall make available, in a manner that is clear and readily available, a statement  
201 summarizing the types of high-risk artificial intelligence systems that are currently deployed or used by  
202 a deployer and how such deployer manages any reasonably foreseeable risk of algorithmic  
203 discrimination that may arise from use or deployment of each high-risk artificial intelligence system  
204 described in this section.

205 **§ 59.1-607. Exemptions.**

206 A. Nothing in this chapter shall be construed to restrict a developer's, deployer's, search engine  
207 operator's, or social media platform operator's ability to (i) comply with federal, state, or municipal  
208 ordinances or regulations; (ii) comply with a civil, criminal, or regulatory inquiry, investigation,  
209 subpoena, or summons by federal, state, municipal, or other governmental authorities; (iii) cooperate  
210 with law-enforcement agencies concerning conduct or activity that the developer, deployer, search  
211 engine operator, or social media platform operator reasonably and in good faith believes may violate  
212 federal, state, or municipal ordinances or regulations; (iv) investigate, establish, exercise, prepare for,  
213 or defend legal claims; (v) provide a product or service specifically requested by a consumer; (vi)  
214 perform under a contract to which a consumer is a party, including fulfilling the terms of a written  
215 warranty; (vii) take steps at the request of a consumer prior to entering into a contract; (viii) take  
216 immediate steps to protect an interest that is essential for the life or physical safety of the consumer or  
217 another individual; (ix) prevent, detect, protect against, or respond to security incidents, identity theft,  
218 fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or  
219 security of systems, or investigate, report, or prosecute those responsible for any such action; (x) engage  
220 in public or peer-reviewed scientific or statistical research in the public interest that adheres to all  
221 other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional  
222 review board that determines, or similar independent oversight entities that determine, (a) that the  
223 expected benefits of the research outweigh the risks associated with such research and (b) whether the  
224 developer, deployer, search engine operator, or social media platform operator has implemented  
225 reasonable safeguards to mitigate the risks associated with such research; (xi) assist another developer,  
226 deployer, search engine operator, or social media platform operator with any of the obligations imposed  
227 by this chapter; or (xii) take any action that is in the public interest in the areas of public health,  
228 community health, or population health, but solely to the extent that such action is subject to suitable  
229 and specific measures to safeguard the public.

230 B. The obligations imposed on developers, deployers, search engine operators, or social media  
231 platform operators by this chapter shall not restrict a developer's, deployer's, search engine operator's,  
232 or social media platform operator's ability to (i) conduct internal research to develop, improve, or  
233 repair products, services, or technologies; (ii) effectuate a product recall; (iii) identify and repair  
234 technical errors that impair existing or intended functionality; or (iv) perform internal operations that  
235 are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the  
236 consumer's existing relationship with the developer, deployer, search engine operator, or social media  
237 platform operator.

238 C. The obligations imposed on developers, deployers, search engine operators, or social media  
239 platform operators by this chapter shall not apply where compliance by the developer, deployer, search  
240 engine operator, or social media platform operator with such obligations would violate an evidentiary  
241 privilege under the laws of the Commonwealth.

242 D. Nothing this chapter shall be construed to impose any obligation on a developer, deployer, search  
243 engine operator, or social media platform operator that adversely affects the rights or freedoms of any

person, including the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution or under the Virginia Human Rights Act (§ 2.2-3900 et seq.).

E. If a developer, deployer, search engine operator, or social media platform operator engages in any action pursuant to an exemption set forth in this section, the developer, deployer, search engine operator, or social media platform operator bears the burden of demonstrating that such action qualifies for such exemption.

**§ 59.1-608. Enforcement; civil penalty.**

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

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

C. Notwithstanding any contrary provision of law, the Attorney General may cause an action to be brought in the appropriate circuit court in the name of the Commonwealth to enjoin any violation of this chapter. The circuit court having jurisdiction may enjoin such violation notwithstanding the existence of an adequate remedy at law. In any action brought pursuant to this section, it shall not be necessary that damages be proved.

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

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

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

**2. That the provisions of § 59.1-606 of the Code of Virginia, as created by this act, shall become effective on July 1, 2026.**