

WEST VIRGINIA LEGISLATURE

2024 REGULAR SESSION

Introduced

House Bill 5338

FISCAL
NOTE

By Delegates Linville, Cannon, Young, W. Clark,
Butler, Ward, Hillenbrand, Brooks, Adkins, Hanshaw
(Mr. Speaker), and Chiarelli

[Introduced on ; Referred
to the Committee on]

1 A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new article,
 2 designated §31A-8H-1, §31A-8H-2, §31A-8H-3, §31A-8H-4, and §31A-8H-5; and by
 3 adding thereto a new article, designated §46A-6O-1, §46A-6O-2, §46A-6O-3, §46A-6O-4,
 4 §46A-6O-5, §46A-6O-6, §46A-6O-7, §46A-6O-8, §46A-6O-9, §46A-6O-10, §46A-6O-11,
 5 §46A-6O-12 and §46A-6O-13, all relating to the Consumer Data Protection Act; inserting
 6 establishing a framework for controlling and processing personal data in the state; creating
 7 definitions; limiting application to all persons that conduct business in the state and either
 8 control or process personal data of at least 100,000 consumers or derive over 50 percent
 9 of gross revenue from the sale of personal data and control or process personal data of at
 10 least 25,000 consumers; providing exemptions; delineating responsibilities and privacy
 11 protection standards for data controllers and processors; clarifying standards do not apply
 12 to state or local governmental entities; providing exceptions for certain types of data and
 13 information governed by federal law; providing that consumers have rights to access,
 14 correct, delete, obtain a copy of personal data, and to opt out of the processing of personal
 15 data for the purposes of targeted advertising; providing that the Attorney General has
 16 exclusive authority to enforce violations of the law; providing for assistance of the Attorney
 17 General in obtaining relief; establishing the Consumer Privacy Fund is created to support
 18 this effort; and providing for construction and an effective date.

Be it enacted by the Legislature of West Virginia:

CHAPTER 31A. BANKS AND BANKING.

ARTICLE 8H. SAFE HARBOR FOR CYBERSECURITY PROGRAMS.

§31A-8H-1. Definitions.

1 As used in this article:

2 (1) "Business" means any limited liability company, limited liability partnership, corporation,
 3 sole proprietorship, association, or other group, however organized and whether operating for

4 profit or not for profit, including a financial institution organized, chartered, or holding a license
5 authorizing operation under the laws of this state, any other state, the United States, or any other
6 country, or the parent or subsidiary of any of the foregoing.

7 "Business" does not include any body, authority, board, bureau, commission, district, or
8 agency of the state or of any political subdivision of the state.

9 (2) "Contract" means the total legal obligation resulting from the parties' agreement as
10 affected by this article and other applicable law.

11 (3) "Covered entity" means a business that accesses, maintains, communicates, or
12 processes personal information or restricted information in or through one or more systems,
13 networks, or services located in or outside this state.

14 (4) "Data breach" means unauthorized access to and acquisition of computerized data that
15 compromises the security or confidentiality of personal information or restricted information owned
16 by or licensed to a covered entity and that causes, reasonably is believed to have caused, or
17 reasonably is believed will cause a material risk of identity theft or other fraud to person or
18 property. "Data breach" does not include either of the following:

19 (A) Good faith acquisition of personal information or restricted information by the covered
20 entity's employee or agent for the purposes of the covered entity provided that the personal
21 information or restricted information is not used for an unlawful purpose or subject to further
22 unauthorized disclosure;

23 (B) Acquisition of personal information or restricted information pursuant to a search
24 warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory
25 state agency.

26 (5) "Distributed ledger technology" means an electronic ledger or other record of
27 transactions or other data to which all of the following apply:

28 (A) The electronic ledger is uniformly ordered.

29 (B) The electronic ledger is redundantly maintained or processed by more than one

1 computer or machine to guarantee the consistency or nonrepudiation of the recorded transactions
2 or other data.

3 (6) "Electronic record" means a record created, generated, sent, communicated, received,
4 or stored by electronic means.

5 (7) "Encryption" means the use of an algorithmic process to transform data into a form in
6 which there is a low probability of assigning meaning without use of a confidential process or key.

7 (8) "Individual" means a natural person.

8 (9) "Maximum probable loss" means the greatest damage expectation that could
9 reasonably occur from a data breach. For purposes of this subsection, "damage expectation"
10 means the total value of possible damage multiplied by the probability that damage would occur.

11 (10)(A) "Personal information" means any information relating to an individual who can be
12 identified, directly or indirectly, in particular by reference to an identifier such as a name, an
13 identification number, social security number, driver's license number or state identification card
14 number, passport number, account number or credit or debit card number, location data, biometric
15 data, an online identifier, or to one or more factors specific to the physical, physiological, genetic,
16 mental, economic, cultural, or social identity of that individual.

17 (B) "Personal information" does not include publicly available information that is lawfully
18 made available to the general public from federal, state, or local government records or any of the
19 following media that are widely distributed:

20 (i) Any news, editorial, or advertising statement published in any bona fide newspaper,
21 journal, or magazine, or broadcast over radio, television, or the internet.

22 (ii) Any gathering or furnishing of information or news by any bona fide reporter,
23 correspondent, or news bureau to news media identified in this paragraph.

24 (iii) Any publication designed for and distributed to members of any bona fide association
25 or charitable or fraternal nonprofit business.

26 (iv) Any type of media similar in nature to any item, entity, or activity identified in this

27 paragraph.

28 (11) "Record" means information that is inscribed on a tangible medium or that is stored in
29 an electronic or other medium and is retrievable in perceivable form.

30 (12) "Redacted" means altered or truncated so that no more than the last four digits of a
31 social security number, driver's license number, state identification card number, account number,
32 or credit or debit card number is accessible as part of the data.

33 (13) "Restricted information" means any information about an individual, other than
34 personal information, or business that, alone or in combination with other information, including
35 personal information, can be used to distinguish or trace the identity of the individual or business,
36 or that is linked or linkable to an individual or business, if the information is not encrypted,
37 redacted, tokenized, or altered by any method or technology in such a manner that the information
38 is anonymized, and the breach of which is likely to result in a material risk of identity theft or other
39 fraud to person or property.

40 (14) "Smart contract" means an electronic record that is an event-driven program or
41 computerized transaction protocol that runs on a distributed, decentralized, shared, and replicated
42 ledger that executes the term of a contract, including but not limited to, taking custody over and
43 instructing the transfer of assets.

44 (15) "Transaction" means a sale, trade, exchange, transfer, payment, or conversion of
45 virtual currency or other digital asset or any other property or any other action or set of actions
46 occurring between two or more persons relating to the conduct of business, commercial, or
47 governmental affairs.

§31A-8H-2. Affirmative defenses.

1 (a) A covered entity seeking an affirmative defense under this chapter shall create,
2 maintain, and comply with a written cybersecurity program that contains administrative, technical,
3 operational, and physical safeguards for the protection of both personal information and restricted
4 information

1 (b) A covered entity's cybersecurity program shall be designed to do all of the following:

2 (1) Continually evaluate and mitigate any reasonably anticipated internal or external
3 threats or hazards that could lead to a data breach.

4 (2) Periodically evaluate no less than annually the maximum probable loss attainable from
5 a data breach.

6 (3) Communicate to any affected parties the extent of any risk posed and any actions the
7 affected parties could take to reduce any damages if a data breach is known to have occurred.

8 (c) The scale and scope of a covered entity's cybersecurity program is appropriate if the
9 cost to operate the cybersecurity program is no less than the covered entity's most recently
10 calculated maximum probable loss value.

11 (d)(1) A covered entity that satisfies all requirements of this section is entitled to an
12 affirmative defense to any cause of action sounding in tort that is brought under the laws of this
13 state or in the courts of this state and that alleges that the failure to implement reasonable
14 information security controls resulted in a data breach concerning personal information or
15 restricted information.

16 (2) A covered entity satisfies all requirements of this section if its cybersecurity program
17 reasonably conforms to an industry-recognized cybersecurity framework, as described in §31A-
18 8H-3 of this code.

§31A-8H-3. Cybersecurity program framework.

1 (a) A covered entity's cybersecurity program, as described in section §31A-8H-2 of this
2 code, reasonably conforms to an industry-recognized cybersecurity framework for purposes of
3 this article if any of the following are true:

4 (1)(A) The cybersecurity program reasonably conforms to the current version of any of the
5 following or any combination of the following, subject to paragraph (B) of this subdivision and
6 subsection (b) of this section:

7 (i) The framework for improving critical infrastructure cybersecurity developed by the

8 national institute of standards and technology.

9 (ii) National institute of standards and technology special publication 800-171.

10 (iii) National institute of standards and technology special publications 800-53 and 800-
11 53a.

12 (iv) The federal risk and authorization management program security assessment
13 framework.

14 (v) The center for internet security critical security controls for effective cyber defense.

15 (vi) The international organization for standardization/international electrotechnical
16 commission 27000 family — information security management systems.

17 (vii) The Cybersecurity Maturity Model Certification at a minimum of Level 2 with external
18 certification.

19 (B) When a final revision to a framework listed in paragraph (A) is published, a covered
20 entity whose cybersecurity program reasonably conforms to that framework shall reasonably
21 conform the elements of its cybersecurity program to the revised framework within the time frame
22 provided in the relevant framework upon which the covered entity intends to rely to support its
23 affirmative defense, but in no event later than one year after the publication date stated in the
24 revision.

25 (2)(A) The covered entity is regulated by the state, by the federal government, or both, or is
26 otherwise subject to the requirements of any of the laws or regulations listed below, and the
27 cybersecurity program reasonably conforms to the entirety of the current version of any of the
28 following, subject to paragraph (B) of this subdivision:

29 (i) The security requirements of the federal Health Insurance Portability and Accountability
30 Act of 1996, as set forth in 45 C.F.R. pt. 164, subpt. C.

31 (ii) Title V of the federal Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as
32 amended.

33 (iii) The federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

1 (iv) The federal Health Information Technology for Economic and Clinical Health Act as set
2 forth in 45 C.F.R. pt. 162.

3 (v) Any applicable rules, regulations, or guidelines for critical infrastructure protection
4 adopted by the federal environmental protection agency, the federal cybersecurity and
5 infrastructure security agency, or the north American reliability corporation.

6 (B) When a framework listed in paragraph (A) of this subdivision is amended, a covered
7 entity whose cybersecurity program reasonably conforms to that framework shall reasonably
8 conform the elements of its cybersecurity program to the amended framework within the time
9 frame provided in the relevant framework upon which the covered entity intends to rely to support
10 its affirmative defense, but in no event later than one year after the effective date of the amended
11 framework.

12 (3)(A) The cybersecurity program reasonably complies with both the current version of the
13 payment card industry data security standard and conforms to the current version of another
14 applicable industry-recognized cybersecurity framework listed in subdivision (a)(1) of this section,
15 subject to paragraph (B) of this subdivision and subsection (b) of this section.

16 (B) When a final revision to the payment card industry data security standard is published,
17 a covered entity whose cybersecurity program reasonably complies with that standard shall
18 reasonably comply the elements of its cybersecurity program with the revised standard within the
19 time frame provided in the relevant framework upon which the covered entity intends to rely to
20 support its affirmative defense, but not later than the effective date for compliance.

21 (b) If a covered entity's cybersecurity program reasonably conforms to a combination of
22 industry-recognized cybersecurity frameworks and two or more of those frameworks are revised,
23 the covered entity whose cybersecurity program reasonably conforms to or complies with, as
24 applicable, those frameworks shall reasonably conform the elements of its cybersecurity program
25 to or comply with, as applicable, all of the revised frameworks within the time frames provided in
26 the relevant frameworks but in no event later than one year after the latest publication date stated

27 in the revisions.

§31A-8H-4. Limitation on private right of action.

1 This article shall not be construed to provide a private right of action, including a class
2 action, with respect to any act or practice regulated therein.

§31A-8H-5. Security assessments; limitation on liability.

1 (a) Any institution of higher education in this state may offer a cybersecurity assessment
2 program as part of an undergraduate or graduate program relating to cybersecurity to any
3 business in the state.

4 (b) An institution of higher education in this state, or any employee or student thereof,
5 offering a cybersecurity assessment program shall be immune from civil liability that arises from
6 the failure of a covered entity to conform to the provisions of this article.

**CHAPTER 46A. WEST VIRGINIA CONSUMER CREDIT AND
PROTECTION ACT.**

ARTICLE 60. CONSUMER DATA PROTECTION ACT.

§46A-60-1. Definitions.

1 As used in this article, unless the context requires a different meaning:

2 "Affiliate" means a legal entity that controls, is controlled by, or is under common control
3 with another legal entity or shares common branding with another legal entity. For the purposes of
4 this definition, "control" or "controlled" means:

5 (1) Ownership of, or the power to vote, more than 50 percent of the outstanding shares of
6 any class of voting security of a company;

7 (2) Control in any manner over the election of a majority of the directors or of individuals
8 exercising similar functions; or

9 (3) The power to exercise controlling influence over the management of a company.

10 "Authenticate" means verifying through reasonable means that the consumer, entitled to

11 exercise his consumer rights in §46A-6O-3 of this code, is the same consumer exercising such
12 consumer rights with respect to the personal data at issue.

13 "Biometric data" means data generated by automatic measurements of an individual's
14 biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique
15 biological patterns or characteristics that is used to identify a specific individual. "Biometric data"
16 does not include a physical or digital photograph, a video or audio recording or data generated
17 therefrom, or information collected, used, or stored for health care treatment, payment, or
18 operations under HIPAA.

19 "Business associate" means the same meaning as the term established by HIPAA.

20 "Child" means any natural person younger than 13 years of age.

21 "Consent" means a clear affirmative act signifying a consumer's freely given, specific,
22 informed, and unambiguous agreement to process personal data relating to the consumer.
23 Consent may include a written statement, including a statement written by electronic means, or
24 any other unambiguous affirmative action. Consent does not include consent induced by use of a
25 user interface designed or manipulated with the substantial effect of subverting or impairing user
26 autonomy, decision-making, or choice.

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

30 "Controller" means the natural or legal person that, alone or jointly with others, determines
31 the purpose and means of processing personal data.

32 "Covered entity" means the same as the term is established by HIPAA.

33 "Decisions that produce legal or similarly significant effects concerning a consumer"
34 means a decision made by the controller that results in the provision or denial by the controller of
35 financial and lending services, housing, insurance, education enrollment, criminal justice,
36 employment opportunities, health care services, or access to basic necessities, such as food and

1 water.

2 "De-identified data" means data that cannot reasonably be linked to an identified or
3 identifiable natural person, or a device linked to such person. A controller that possesses "de-
4 identified data" shall comply with the requirements of subsection (a) of §46A-6O-7.

5 "Fund" means the Consumer Privacy Fund established pursuant to §46A-6O-11 of this
6 code.

7 "Health record" means any written, printed or electronically recorded material maintained
8 by a health care entity in the course of providing health services to an individual concerning the
9 individual and the services provided. "Health record" also includes the substance of any
10 communication made by an individual to a health care entity in confidence during or in connection
11 with the provision of health services or information otherwise acquired by the health care entity
12 about an individual in confidence and in connection with the provision of health services to the
13 individual.

14 "Health care provider" means the same as that term is defined in §16-30-3 of this code.

15 "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42
16 U.S.C. §1320d *et seq.*).

17 "Identified or identifiable natural person" means a person who can be readily identified,
18 directly or indirectly.

19 "Institution of higher education" means a state institution of higher education as defined in
20 §18B-1-2 of this code and, includes further, any private institution of higher education.

21 "Nonprofit organization" means any corporation organized under the West Virginia
22 Nonprofit Corporation Act, Chapter §31-1-101 of this code, *et seq.*, or any organization exempt
23 from taxation under §§501(c)(3), 501(c)(6), or 501 (c)(12) of the Internal Revenue Code.

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

1

2 "Precise geolocation data" means information derived from technology, including, but not
3 limited to, global positioning system level latitude and longitude coordinates or other mechanisms,
4 that directly identifies the specific location of a natural person with precision and accuracy within a
5 radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or
6 any data generated by or connected to advanced utility metering infrastructure systems or
7 equipment for use by a utility.

8 "Process" or "processing" means any operation or set of operations performed, whether by
9 manual or automated means, on personal data or on sets of personal data, such as the collection,
10 use, storage, disclosure, analysis, deletion, or modification of personal data.

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

13 "Profiling" means any form of automated processing performed on personal data to
14 evaluate, analyze, or predict personal aspects related to an identified or identifiable natural
15 person's economic situation, health, personal preferences, interests, reliability, behavior, location,
16 or movements.

17 "Protected health information" means the same as the term is established by HIPAA.

18 "Pseudonymous data" means personal data that cannot be attributed to a specific natural
19 person without the use of additional information, provided that such additional information is kept
20 separately and is subject to appropriate technical and organizational measures to ensure that the
21 personal data is not attributed to an identified or identifiable natural person.

22 "Publicly available information" means information that is lawfully made available through
23 federal, state, or local government records, or information that a business has a reasonable basis
24 to believe is lawfully made available to the general public through widely distributed media, by the
25 consumer, or by a person to whom the consumer has disclosed the information, unless the
26 consumer has restricted the information to a specific audience.

1 "Sale of personal data" means the exchange of personal data for any form of valuable
2 consideration, including but not limited to, monetary consideration by the controller to any third
3 party. "Sale of personal data" does not include:

4 (1) The disclosure of personal data to a processor that processes the personal data on
5 behalf of the controller;

6 (2) The disclosure of personal data to a third party for purposes of providing a product or
7 service requested by the consumer;

8 (3) The disclosure or transfer of personal data to an affiliate of the controller;

9 (4) The disclosure of information that the consumer (i) intentionally made available to the
10 general public via a channel of mass media and (ii) did not restrict to a specific audience; or

11 (5) The disclosure or transfer of personal data to a third party as an asset that is part of a
12 merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all
13 or part of the controller's assets.

14 "Sensitive data" means a category of personal data that includes:

15 (1) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical
16 health diagnosis, sexual orientation, or citizenship or immigration status;

17 (2) The processing of genetic or biometric data for the purpose of uniquely identifying a
18 natural person;

19 (3) The personal data collected from a known child; or

20 (4) Precise geolocation data.

21 "State agency" means the same as that term is defined in §6D-1-1 of this code and

22 "Targeted advertising" means displaying advertisements to a consumer where the
23 advertisement is selected based on personal data obtained from that consumer's activities over
24 time and across nonaffiliated websites or online applications to predict such consumer's
25 preferences or interests. "Targeted advertising" does not include:

26 (1) Advertisements based on activities within a controller's own websites or online

1 applications;

2 (2) Advertisements based on the context of a consumer's current search query, visit to a
3 website, or online application;

4 (3) Advertisements directed to a consumer in response to the consumer's request for
5 information or feedback; or

6 (4) Processing personal data processed solely for measuring or reporting advertising
7 performance, reach, or frequency.

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

10 "Trade secret" means information, without regard to form, including, but not limited to,
11 technical, nontechnical, or financial data, a formula, pattern, compilation, program, device,
12 method, technique, plan, or process, that:

13 (1) Derives independent economic value, actual or potential, from not being generally
14 known to, and not being readily ascertainable by proper means by, other persons who can obtain
15 economic value from the information's disclosure or use; and

16 (2) Is the subject of efforts that are reasonable under the circumstances to maintain the
17 information's secrecy.

§46A-60-2. Scope; exemptions.

18 (a) This article applies to persons that conduct business in the state or produce products or
19 services that are targeted to residents of the state and that

20 (1) During a calendar year, control or process personal data of at least 100,000
21 consumers;

22 (2) Control or process personal data of at least 25,000 consumers and derive over 50
23 percent of gross revenue from the sale of personal data; or

24 (3) Have annual gross revenues generated in this state which exceed \$25,000,000.

25 (b) This article shall not apply to any:

26 (1) Body, authority, board, bureau, commission, district, or agency of the state or of any
27 political subdivision of the state;

28 (2) Financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act
29 (15 U.S.C. §6801 et seq.);

30 (3) Covered entity or business associate governed by the privacy, security, and breach
31 notification rules issued by the United States Department of Health and Human Services, 45
32 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology
33 for Economic and Clinical Health Act (Public Law 111-5);

34 (4) Nonprofit organization; or

35 (5) Institution of higher education.

36 (c) The following information and data is exempt from this article:

37 (1) Protected health information under HIPAA;

38 (2) Health records for purposes of Title 32.1;

39 (3) Patient identifying information for purposes of 42 U.S.C. §290dd-2;

40 (4) Identifiable private information for purposes of the federal policy for the protection of
41 human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise
42 information collected as part of human subjects research pursuant to the good clinical practice
43 guidelines issued by The International Council for Harmonisation of Technical Requirements for
44 Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50,
45 and 56, or personal data used or shared in research conducted in accordance with the
46 requirements set forth in this chapter, or other research conducted in accordance with applicable
47 law;

48 (5) Information and documents created for purposes of the federal Health Care Quality
49 Improvement Act of 1986 (42 U.S.C. §11101 et seq.);

50 (6) Patient safety work product for purposes of the federal Patient Safety and Quality
51 Improvement Act (42 U.S.C. §299b-21 et seq.);

52 (7) Information derived from any of the health care-related information listed in this
53 subsection that is de-identified in accordance with the requirements for de-identification pursuant
54 to HIPAA;

55 (8) Information originating from, and intermingled to be indistinguishable with, or
56 information treated in the same manner as information exempt under this subsection that is
57 maintained by a covered entity or business associate as defined by HIPAA or a program or a
58 qualified service organization as defined by 42 U.S.C.§290dd-2;

59 (9) Information used only for public health activities and purposes as authorized by HIPAA;

60 (10) The collection, maintenance, disclosure, sale, communication, or use of any personal
61 information bearing on a consumer's credit worthiness, credit standing, credit capacity, character,
62 general reputation, personal characteristics, or mode of living by a consumer reporting agency,
63 furnisher, or user that provides information for use in a consumer report, and by a user of a
64 consumer report, but only to the extent that such activity is regulated by and authorized under the
65 federal Fair Credit Reporting Act (15 U.S.C.§1681 et seq.);

66 (11) Personal data collected, processed, sold, or disclosed in compliance with the federal
67 Driver's Privacy Protection Act of 1994 (18 U.S.C.§2721 et seq.);

68 (12) Personal data regulated by the federal Family Educational Rights and Privacy Act (20
69 U.S.C.§1232g et seq.);

70 (13) Personal data collected, processed, sold, or disclosed in compliance with the federal
71 Farm Credit Act (12 U.S.C.§2001 et seq.); and

72 (14) Data processed or maintained:

73 (A) In the course of an individual applying to, employed by, or acting as an agent or
74 independent contractor of a controller, processor, or third party, to the extent that the data is
75 collected and used within the context of that role;

76 (B) As the emergency contact information of an individual under this chapter used for
77 emergency contact purposes; or

78 (C) That is necessary to retain to administer benefits for another individual relating to the
79 individual under §46A-6O-2(c)(14)(A) of this code and used for the purposes of administering
80 those benefits.

81 (d) Controllers and processors that comply with the verifiable parental consent
82 requirements of the Children's Online Privacy Protection Act (15 U.S.C. §6501 et seq.) shall be
83 deemed compliant with any obligation to obtain parental consent under this chapter.

84 (e) No provision of this article shall be construed as requiring a controller, processor, third
85 party, or consumer to disclose any trade secrets.

§46A-6O-3. Personal data rights; consumers.

1 (a) A consumer may invoke the consumer rights authorized pursuant to this subsection at
2 any time by submitting a request to a controller specifying the consumer rights the consumer
3 wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on
4 behalf of the child regarding processing personal data belonging to the known child. A controller
5 shall comply with an authenticated consumer request to exercise the right:

6 (1) To confirm whether or not a controller is processing the consumer's personal data and
7 to access such personal data;

8 (2) To correct inaccuracies in the consumer's personal data, taking into account the nature
9 of the personal data and the purposes of the processing of the consumer's personal data;

10 (3) To delete personal data provided by or obtained about the consumer;

11 (4) To obtain a copy of the consumer's personal data that the consumer previously
12 provided to the controller in a portable and, to the extent technically feasible, readily usable format
13 that allows the consumer to transmit the data to another controller without hindrance, where the
14 processing is carried out by automated means; and

15 (5) To opt out of the processing of the personal data for purposes of:

16 (A) Targeted advertising;

17 (B) The sale of personal data; or

18 (C) Profiling in furtherance of decisions that produce legal or similarly significant effects
19 concerning the consumer.

20 (b) Except as otherwise provided in this chapter, a controller shall comply with a request by
21 a consumer to exercise the consumer rights authorized pursuant to the provisions of §46A-6O-
22 3(a) of this code as follows:

23 (1) A controller shall respond to the consumer without undue delay, but in all cases within
24 45 days of receipt of the request submitted pursuant to the methods described in §46A-6O-3(a) of
25 this code. The response period may be extended once by 45 additional days when reasonably
26 necessary, taking into account the complexity and number of the consumer's requests, so long as
27 the controller informs the consumer of any such extension within the initial 45-day response
28 period, together with the reason for the extension.

29 (2) If a controller declines to take action regarding the consumer's request, the controller
30 shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of
31 receipt of the request, of the justification for declining to take action and instructions for how to
32 appeal the decision pursuant to §46A-6O-3(c) of this code.

33 (3) Information provided in response to a consumer request shall be provided by a
34 controller free of charge, up to twice annually per consumer. If requests from a consumer are
35 manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a
36 reasonable fee to cover the administrative costs of complying with the request or decline to act on
37 the request. The controller bears the burden of demonstrating the manifestly unfounded,
38 excessive, or repetitive nature of the request.

39 (4) If a controller is unable to authenticate the request using commercially reasonable
40 efforts, the controller shall not be required to comply with a request to initiate an action under
41 subsection (a) of this section and may request that the consumer provide additional information
42 reasonably necessary to authenticate the consumer and the consumer's request.

43 (c) A controller shall establish a process for a consumer to appeal the controller's refusal to

44 take action on a request within a reasonable period of time after the consumer's receipt of the
45 decision pursuant to §46A-6O-3(b)(2) of this code. The appeal process shall be conspicuously
46 available and similar to the process for submitting requests to initiate action pursuant to §46A-6O-
47 3(a) of this code. Within 60 days of receipt of an appeal, a controller shall inform the consumer in
48 writing of any action taken or not taken in response to the appeal, including a written explanation of
49 the reasons for the decisions. If the appeal is denied, the controller shall also provide the
50 consumer with an online mechanism, if available, or other method through which the consumer
51 may contact the Attorney General to submit a complaint.

§46A-6O-4. Data controller responsibilities; transparency.

1 (a) A controller shall:

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

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

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

13 (4) Not process personal data in violation of state and federal laws that prohibit unlawful
14 discrimination against consumers. A controller shall not discriminate against a consumer for
15 exercising any of the consumer rights contained in this chapter, including denying goods or
16 services, charging different prices or rates for goods or services, or providing a different level of
17 quality of goods and services to the consumer. However, nothing in this subdivision shall be

18 construed to require a controller to provide a product or service that requires the personal data of a
19 consumer that the controller does not collect or maintain or to prohibit a controller from offering a
20 different price, rate, level, quality, or selection of goods or services to a consumer, including
21 offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to
22 §46A-6O-3 of this code or the offer is related to a consumer's voluntary participation in a bona fide
23 loyalty, rewards, premium features, discounts, or club card program; and

24 (5) Not process sensitive data concerning a consumer without obtaining the consumer's
25 consent, or, in the case of the processing of sensitive data concerning a known child, without
26 processing such data in accordance with the federal Children's Online Privacy Protection Act (15
27 U.S.C. §6501 *et seq.*).

28 (b) Any provision of a contract or agreement of any kind that purports to waive or limit in
29 any way consumer rights pursuant to §46A-6O-3 of this code shall be deemed contrary to public
30 policy and shall be void and unenforceable.

31 (c) Controllers shall provide consumers with a reasonably accessible, clear, and
32 meaningful privacy notice that includes:

33 (1) The categories of personal data processed by the controller;

34 (2) The purpose for processing personal data;

35 (3) How consumers may exercise their consumer rights pursuant to §46A-6O-3 of this
36 code, including how a consumer may appeal a controller's decision with regard to the consumer's
37 request;

38 (4) The categories of personal data that the controller shares with third parties, if any; and

39 (5) The categories of third parties, if any, with whom the controller shares personal data.

40 (d) If a controller sells personal data to third parties or processes personal data for targeted
41 advertising, the controller shall clearly and conspicuously disclose such processing, as well as the
42 manner in which a consumer may exercise the right to opt out of such processing.

43 (e) A controller shall establish, and shall describe in a privacy notice, one or more secure

44 and reliable means for consumers to submit a request to exercise their consumer rights under this
45 chapter. Such means shall take into account the ways in which consumers normally interact with
46 the controller, the need for secure and reliable communication of such requests, and the ability of
47 the controller to authenticate the identity of the consumer making the request. Controllers shall not
48 require a consumer to create a new account in order to exercise consumer rights pursuant to
49 §46A-6O-3 of this code but may require a consumer to use an existing account.

§46A-6O-5. Responsibility according to role; controller and processor.

1 (a) A processor shall adhere to the instructions of a controller and shall assist the controller
2 in meeting its obligations under this chapter. Such assistance shall include:

3 (1) Taking into account the nature of processing and the information available to the
4 processor, by appropriate technical and organizational measures, insofar as this is reasonably
5 practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to
6 the provisions of §46A-6O-3 of this code;

7 (2) Taking into account the nature of processing and the information available to the
8 processor, by assisting the controller in meeting the controller's obligations in relation to the
9 security of processing the personal data and in relation to the notification of a breach of security of
10 the system of the processor pursuant to §46-2A-102 of this code in order to meet the controller's
11 obligations;

12 (3) Providing necessary information to enable the controller to conduct and document data
13 protection assessments pursuant to the provisions of §46A-6O-6 of this code.

14 (b) A contract between a controller and a processor shall govern the processor's data
15 processing procedures with respect to processing performed on behalf of the controller. The
16 contract shall be binding and clearly set forth instructions for processing data, the nature and
17 purpose of processing, the type of data subject to processing, the duration of processing, and the
18 rights and obligations of both parties. The contract shall also include requirements that the
19 processor shall:

20 (1) Ensure that each person processing personal data is subject to a duty of confidentiality
21 with respect to the data;

22 (2) At the controller's direction, delete or return all personal data to the controller as
23 requested at the end of the provision of services, unless retention of the personal data is required
24 by law;

25 (3) Upon the reasonable request of the controller, make available to the controller all
26 information in its possession necessary to demonstrate the processor's compliance with the
27 obligations in this chapter;

28 (4) Allow, and cooperate with, reasonable assessments by the controller or the controller's
29 designated assessor; alternatively, the processor may arrange for a qualified and independent
30 assessor to conduct an assessment of the processor's policies and technical and organizational
31 measures in support of the obligations under this chapter using an appropriate and accepted
32 control standard or framework and assessment procedure for such assessments. The processor
33 shall provide a report of such assessment to the controller upon request; and

34 (5) Engage any subcontractor pursuant to a written contract in accordance with subsection
35 (c) of this section that requires the subcontractor to meet the obligations of the processor with
36 respect to the personal data.

37 (c) Nothing in this section shall be construed to relieve a controller or a processor from the
38 liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

39 (d) Determining whether a person is acting as a controller or processor with respect to a
40 specific processing of data is a fact-based determination that depends upon the context in which
41 personal data is to be processed. A processor that continues to adhere to a controller's
42 instructions with respect to a specific processing of personal data remains a processor.

§46A-60-6. Data protection assessments.

1 (a) A controller shall conduct and document a data protection assessment of each of the
2 following processing activities involving personal data:

- 3 (1) The processing of personal data for purposes of targeted advertising;
4 (2) The sale of personal data;
5 (3) The processing of personal data for purposes of profiling, where such profiling presents
6 a reasonably foreseeable risk of:
7 (A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
8 (B) Financial, physical, or reputational injury to consumers;
9 (C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or
10 concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
11 (D) Other substantial injury to consumers;
12 (4) The processing of sensitive data; and
13 (5) Any processing activities involving personal data that present a heightened risk of harm
14 to consumers.
- 15 (b) Data protection assessments conducted pursuant to §46A-6O-6(a) of this code shall
16 identify and weigh the benefits that may flow, directly and indirectly, from the processing to the
17 controller, the consumer, other stakeholders, and the public against the potential risks to the rights
18 of the consumer associated with such processing, as mitigated by safeguards that can be
19 employed by the controller to reduce such risks. The use of de-identified data and the reasonable
20 expectations of consumers, as well as the context of the processing and the relationship between
21 the controller and the consumer whose personal data will be processed, shall be factored into this
22 assessment by the controller.
- 23 (c) The Attorney General may request, pursuant to an investigative civil demand, that a
24 controller disclose any data protection assessment that is relevant to an investigation conducted
25 by the Attorney General, and the controller shall make the data protection assessment available to
26 the Attorney General. The Attorney General may evaluate the data protection assessment for
27 compliance with the responsibilities set forth in §46A-6O-4 of this code. Data protection
28 assessments shall be confidential and exempt from public inspection and copying under the West

29 Virginia Freedom of Information Act, §29B-1-1, et seq. of this code. The disclosure of a data
30 protection assessment pursuant to a request from the Attorney General shall not constitute a
31 waiver of attorney-client privilege or work product protection with respect to the assessment and
32 any information contained in the assessment.

33 (d) A single data protection assessment may address a comparable set of processing
34 operations that include similar activities.

35 (e) Data protection assessments conducted by a controller for the purpose of compliance
36 with other laws or regulations may comply under this section if the assessments have a
37 reasonably comparable scope and effect.

38 (f) Data protection assessment requirements shall apply to processing activities created or
39 generated after January 1, 2024, and are not retroactive.

§46A-6O-7. Processing de-identified data; exemptions.

1 (a) The controller in possession of de-identified data shall:

2 (1) Take reasonable measures to ensure that the data cannot be associated with a natural
3 person;

4 (2) Publicly commit to maintaining and using de-identified data without attempting to re-
5 identify the data; and

6 (3) Contractually obligate any recipients of the de-identified data to comply with all
7 provisions of this chapter.

8 (b) Nothing in this chapter shall be construed to require a controller or processor to:

9 (1) Re-identify de-identified data or pseudonymous data; or

10 (2) Maintain data in identifiable form, or collect, obtain, retain, or access any data or
11 technology, in order to be capable of associating an authenticated consumer request with personal
12 data.

13 (c) Nothing in this chapter shall be construed to require a controller or processor to comply
14 with an authenticated consumer rights request, pursuant to §46A-6O-3 of this code, if all of the

15 following are true:

16 (1) The controller is not reasonably capable of associating the request with the personal
17 data or it would be unreasonably burdensome for the controller to associate the request with the
18 personal data;

19 (2) The controller does not use the personal data to recognize or respond to the specific
20 consumer who is the subject of the personal data, or associate the personal data with other
21 personal data about the same specific consumer; and

22 (3) The controller does not sell the personal data to any third party or otherwise voluntarily
23 disclose the personal data to any third party other than a processor, except as otherwise permitted
24 in this section.

25 (d) The consumer rights contained in §46A-6O-3 and §46A-6O-4 of this code do not apply
26 to pseudonymous data in cases where the controller is able to demonstrate any information
27 necessary to identify the consumer is kept separately and is subject to effective technical and
28 organizational controls that prevent the controller from accessing such information.

29 (e) A controller that discloses pseudonymous data or de-identified data shall exercise
30 reasonable oversight to monitor compliance with any contractual commitments to which the
31 pseudonymous data or de-identified data is subject and shall take appropriate steps to address
32 any breaches of those contractual commitments.

§46A-6O-8.

Limitations.

1 (a) Nothing in this article shall be construed to restrict a controller's or processor's ability to:

2 (1) Comply with federal, state, or local laws, rules, or regulations;

3 (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
4 summons by federal, state, local, or other governmental authorities;

5 (3) Cooperate with law-enforcement agencies concerning conduct or activity that the
6 controller or processor reasonably and in good faith believes may violate federal, state, or local
7 laws, rules, or regulations;

8 (4) Investigate, establish, exercise, prepare for, or defend legal claims;

9 (5) Provide a product or service specifically requested by a consumer, perform a contract
10 to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at
11 the request of the consumer prior to entering into a contract;

12 (6) Take immediate steps to protect an interest that is essential for the life or physical safety
13 of the consumer or of another natural person, and where the processing cannot be manifestly
14 based on another legal basis;

15 (7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud,
16 harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or
17 security of systems; or investigate, report, or prosecute those responsible for any such action;

18 (8) Engage in public or peer-reviewed scientific or statistical research in the public interest
19 that adheres to all other applicable ethics and privacy laws and is approved, monitored, and
20 governed by an institutional review board, or similar independent oversight entities that determine:

21 (A) If the deletion of the information is likely to provide substantial benefits that do not
22 exclusively accrue to the controller;

23 (B) The expected benefits of the research outweigh the privacy risks; and

24 (C) If the controller has implemented reasonable safeguards to mitigate privacy risks
25 associated with research, including any risks associated with reidentification; or

26 (D) Assist another controller, processor, or third party with any of the obligations under this
27 subsection.

28 (b) The obligations imposed on controllers or processors under this chapter shall not
29 restrict a controller's or processor's ability to collect, use, or retain data to:

30 (1) Conduct internal research to develop, improve, or repair products, services, or
31 technology;

32 (2) Effectuate a product recall;

33 (3) Identify and repair technical errors that impair existing or intended functionality; or

34 (4) Perform internal operations that are reasonably aligned with the expectations of the
35 consumer or reasonably anticipated based on the consumer's existing relationship with the
36 controller or are otherwise compatible with processing data in furtherance of the provision of a
37 product or service specifically requested by a consumer or the performance of a contract to which
38 the consumer is a party.

39 (c) The obligations imposed on controllers or processors under this chapter shall not apply
40 where compliance by the controller or processor with this chapter would violate an evidentiary
41 privilege under the laws of this state. Nothing in this article shall be construed to prevent a
42 controller or processor from providing personal data concerning a consumer to a person covered
43 by an evidentiary privilege under the laws of the state as part of a privileged communication.

44 (d) A controller or processor that discloses personal data to a third-party controller or
45 processor, in compliance with the requirements of this article, is not in violation of this article if the
46 third-party controller or processor that receives and processes such personal data is in violation of
47 this article, provided that, at the time of disclosing the personal data, the disclosing controller or
48 processor did not have actual knowledge that the recipient intended to commit a violation. A third-
49 party controller or processor receiving personal data from a controller or processor in compliance
50 with the requirements of this article is likewise not in violation of this article for the transgressions
51 of the controller or processor from which it receives such personal data.

52 (e) Nothing in this article shall be construed as an obligation imposed on controllers and
53 processors that adversely affects the rights or freedoms of any persons, such as exercising the
54 right of free speech pursuant to the First Amendment to the United States Constitution, or applies
55 to the processing of personal data by a person in the course of a purely personal or household
56 activity.

57 (f) Personal data processed by a controller pursuant to this section shall not be processed
58 for any purpose other than those expressly listed in this section unless otherwise allowed by this
59 article. Personal data processed by a controller pursuant to this section may be processed to the

60 extent that such processing is:

61 (1) Reasonably necessary and proportionate to the purposes listed in this section; and

62 (2) Adequate, relevant, and limited to what is necessary in relation to the specific purposes
63 listed in this section. Personal data collected, used, or retained pursuant to §46A-6O-8(b) of this
64 code, shall, where applicable, take into account the nature and purpose or purposes of such
65 collection, use, or retention. Such data shall be subject to reasonable administrative, technical,
66 and physical measures to protect the confidentiality, integrity, and accessibility of the personal
67 data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection,
68 use, or retention of personal data.

69 (g) If a controller processes personal data pursuant to an exemption in this section, the
70 controller bears the burden of demonstrating that such processing qualifies for the exemption and
71 complies with the requirements in §46A-6O-8(f) of this code.

72 (h) Processing personal data for the purposes expressly identified in §46A-6O-8(a) of this
73 code shall not solely make an entity a controller with respect to such processing.

§46A-6O-9. Violations of article; civil penalty.

1 (a) The Attorney General shall have exclusive authority to enforce violations of this article.

2 (b) Prior to initiating any action under this article, the Attorney General shall provide a
3 controller or processor 30 days' written notice identifying the specific provisions of this article the
4 Attorney General, on behalf of a consumer, alleges have been or are being violated. If within the
5 30 days the controller or processor cures the noticed violation and provides the Attorney General
6 an express written statement that the alleged violations have been cured and that no further
7 violations shall occur, no action for statutory damages shall be initiated against the controller or
8 processor.

9 (c) If a controller or processor continues to violate this article in breach of an express
10 written statement provided to the consumer under this section, the Attorney General may initiate
11 an action and seek damages for up to \$7,500 for each violation under this chapter.

12 (d) Nothing in this article shall be construed as providing the basis for, or be subject to, a
13 private right of action to violations of this article or under any other law.

§46A-6O-10 Enforcement; civil penalty.

1 (a) The Attorney General retains exclusive authority to enforce this article by bringing an
2 action in the name of the state, or on behalf of persons residing in the state. The Attorney General
3 may issue a civil investigative demand to any controller or processor believed to be engaged in, or
4 about to engage in, any violation of this article. The provisions of §47-18-1 of this code shall apply
5 to civil investigative demands issued under this section.

6 (b) Any controller or processor that violates this article is subject to an injunction and liable
7 for a civil penalty of not more than \$7,500 for each violation.

8 (c) The Attorney General may recover reasonable expenses incurred in investigating and
9 preparing the case, including attorney fees, of any action initiated under this article.

§46A-6O-11. Attorney General's assistance in personal data claims.

1 (a) In order to effectuate the protection of personal data as defined in §46A-6O-1 of this
2 code, the Attorney General shall establish a process whereby a consumer may seek to utilize any
3 of the personal data protections established in §46A-6O-3 of this code through the agency of the
4 Attorney General's Office. This process shall include:

5 (1) An ability to discover what controllers and processors may hold such data about the
6 consumer;

7 (2) An ability to discover what third-party controllers or processors may have received such
8 data about the consumer;

9 (3) An ability to formally request from each controller, third-party controller, processor, and
10 third-party processor copies of the personal data of the requesting person held by those entities,
11 and to call for modification and/or deletion thereof.

12 (b) The Attorney General shall promulgate legislative rules necessary to carry out the
13 provisions of this section.

§46A-60-12. Consumer Privacy Fund.

1 There is hereby created in the state treasury a special nonreverting fund to be known as
2 the Consumer Privacy Fund. The Fund shall be established on the books of the Comptroller. All
3 civil penalties collected pursuant to this article shall be paid into the state treasury and credited to
4 the Fund. Interest earned on moneys in the Fund shall remain in the Fund and be credited to it.
5 Any moneys remaining in the Fund, including interest thereon, at the end of each fiscal year shall
6 not revert to the general fund but shall remain in the Fund. Moneys in the Fund shall be used to
7 support the work of the Office of the Attorney General to enforce the provisions of this article,
8 subject to appropriation.

§46A-60-13. Construction and Enactment.

1 (a) The intent of the Legislature in enacting this article is to establish a statewide,
2 comprehensive enactment that applies to all parts of the state, operating uniformly throughout the
3 state. No political subdivision of this state shall be construed by any provision of this article to be
4 authorized to enact any law regarding the controlling or processing of personal data.

5 (b) Any reference to federal law or statute in this article shall be deemed to include any
6 accompanying rules or regulations or exemptions thereto. Further, this enactment is declaratory of
7 existing law.

8 (c) This article shall become effective on January 1, 2025.

NOTE: The purpose of this bill is to all create the Consumer Data Protection Act; establishing a framework for controlling and processing personal data in the state; creating definitions; limiting application to all persons that conduct business in the state and either control or process personal data of at least 100,000 consumers or derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers; providing for exemptions; delineating responsibilities and privacy protection standards for data controllers and processors; clarifying standards do not apply to state or local governmental entities; providing exceptions for certain types of data and information governed by federal law; providing that consumers have rights to access, correct, delete, obtain a copy of personal data, and to opt out of the processing of personal data for the purposes of targeted advertising; providing that the Attorney General has exclusive authority to enforce violations of the law; providing for assistance of the Attorney General in obtaining relief; establishing the Consumer Privacy Fund to support this effort; and providing for construction and an effective date.

Strike-throughs indicate language that would be stricken from a heading or the present law

and underscoring indicates new language that would be added.