WEST VIRGINIA LEGISLATURE

2025 REGULAR SESSION

Introduced

House Bill 2987

By Delegates Linville, J. Cannon, Moore, and Pritt

Introduced February 26, 2025; referred to the Committee on Energy and Public Works then the Judiciary

A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new article, designated §31A-8H-1, §31A-8H-2, §31A-8H-3, §31A-8H-4, and §31A-8H-5; and to amend said code by adding a new article, designated §46A-6O-1, §46A-6O-2, §46A-6O-3, §46A-6O-4, §46A-6O-5, §46A-6O-6, §46A-6O-7, §46A-6O-8, §46A-6O-9, §46A-6O-10, §46A-6O-11, §46A-6O-12 and §46A-6O-13, relating to the Consumer Data Protection Act; inserting 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% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers; providing 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.

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.

As used in this article:

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

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

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

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

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

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

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

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

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

(A) The electronic ledger is uniformly ordered.

(B) The electronic ledger is redundantly maintained or processed by more than one computer or machine to guarantee the consistency or nonrepudiation of the recorded transactions or other data.

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

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

(8) "Individual" means a natural person.

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

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

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

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

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

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

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

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

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

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

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

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

§31A-8H-2. Affirmative defenses.

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

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

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

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

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

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

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

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

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

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

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

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

National Institute of Standards and Technology.

(ii) National Institute of Standards and Technology special publication 800-171.

(iii) National Institute of Standards and Technology special publications 800-53 and 800-53a.

(iv) The federal Risk and Authorization Management Program security assessment framework.

(v) The Center for Internet Security critical security controls for effective cyber defense.

(vi) The International Organization for Standardization/International Electrotechnical Commission 27000 family — information security management systems.

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

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

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

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

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

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

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

(v) Any applicable rules, regulations, or guidelines for critical infrastructure protection adopted by the federal Environmental Protection Agency, the federal Cybersecurity and Infrastructure Security Agency, or the North American reliability corporation.

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

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

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

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

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

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

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

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

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

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

ARTICLE 6O. CONSUMER DATA PROTECTION ACT.

§46A-6O-1. Definitions.

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

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

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

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

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

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in §46A-6O-3 of this code, is the same consumer exercising such consumer rights with respect to the personal data at issue.

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

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

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

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

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

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

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

"Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Examples of a direct relationship with a business include if the consumer is a past or present:

(1) Customer, client, subscriber, user, or registered user of the business's goods or services;

(2) Employee, contractor, or agent of the business;

(3) Investor in the business; or

(4) Donor to the business.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(4) Precise geolocation data.

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

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

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

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

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

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

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

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

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

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

§46A-6O-2. Scope; exemptions.

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

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

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

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

(b) This article shall not apply to any:

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

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

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

(4) Nonprofit organization; or

(5) Institution of higher education.

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

(1) Protected health information under HIPAA;

(2) Health records for purposes of Title 32.1;

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

(4) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for

Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law;

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

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

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

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

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

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

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

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

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

(14) Data processed or maintained:

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

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

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

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

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

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

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

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

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

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

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

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

(A) Targeted advertising;

(B) The sale of personal data; or

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

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

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

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

(3) Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a

reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

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

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

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

(a) A controller shall:

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

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

(3) Establish, implement, and maintain reasonable administrative, technical, and physical

data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;

(4) Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to §46A-6O-3 of this code or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

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

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

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

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

(2) The purpose for processing personal data;

(3) How consumers may exercise their consumer rights pursuant to §46A-6O-3 of this

code, including how a consumer may appeal a controller's decision with regard to the consumer's request;

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

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

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

(e) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to §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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) The processing of personal data for purposes of targeted advertising;

(2) The sale of personal data;

(3) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) Financial, physical, or reputational injury to consumers;

(C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

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

(b) Data protection assessments conducted pursuant to §46A-6O-6(a) of this code shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

(c) The Attorney General may request, pursuant to an investigative civil demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in §46A-6O-4 of this code. Data protection assessments shall be confidential and exempt from public inspection and copying under the West Virginia Freedom of Information Act, §29B-1-1 *et seq*. of this code. The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

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

(f) Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2025, and are not retroactive.

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

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

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

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

(3) Contractually obligate any recipients of the de-identified data to comply with all

provisions of this chapter.

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

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

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

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

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

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

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

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

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

§46A-6O-8. Limitations.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) Effectuate a product recall;

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

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

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

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

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

(f) Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this article. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

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

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

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

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

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

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

(b) Prior to initiating any action under this article, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this article the

Attorney General, on behalf of a consumer, alleges have been or are being violated. If within the 30 days the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action for statutory damages shall be initiated against the controller or processor.

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

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

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

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

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

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

§46A-6O-11. Data broker registration with the Attorney General.

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in section 46A-6O-1 of this chapter, a data broker shall:

(1) Register with the Attorney General;

(2) Pay a registration fee of $100.00; and

(3) Provide the following information:

(4) The name and primary physical, e-mail, and Internet addresses of the data broker;

(5) In connection with the consumer rights authorized under §46A-6O-3, a data broker must provide the following information regarding the collection of personal information:

(A) The method for requesting to exercise the following consumer rights:

(i)To confirm whether or not a controller is processing the consumer's personal data and

(ii) To access such personal data;

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

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

(B) The method for requesting an opt-out of sale;

(C) Whether the data broker permits a consumer to authorize a third party to perform the opt-out of sale on the consumer's behalf;

(D) A statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(E) A statement whether the data broker implements a purchaser credentialing process;

(F) The number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(G) Where the data broker has actual knowledge that it possesses the personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal information of minors; and

(H) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to the provisions of subsection (a) of this section is liable to the State for:

(1) A civil penalty of $50 for each day, not to exceed a total of $10,000.00 for each year, it fails to register pursuant to this section;

(2) An amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) Other penalties imposed by law.

§46A-6O-12. Consumer Privacy Fund.

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

§46A-6O-13. Construction and Enactment.

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

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

(c) This article shall become effective on January 1, 2026.

NOTE: The purpose of this bill is to create the Consumer Data Protection Act and to provide guidance for the Act's administration.

Strike-throughs indicate language that would be stricken from a heading or the present law and underscoring indicates new language that would be added.