Senate Bill 473

By: Senators Albers of the 56th, Robertson of the 29th, Anavitarte of the 31st, Strickland of the 17th, Goodman of the 8th and others

A BILL TO BE ENTITLED

AN ACT

To amend Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, so as to enact the "Georgia Consumer Privacy Protection Act"; to protect the privacy of consumer personal data in this state; to provide for definitions; to provide for applicability; to provide for exemptions for certain entities, data, and uses of data; to provide for consumer rights regarding personal data; to provide for a consumer to exercise such rights by submitting a request to a controller; to provide for a controller to promptly respond to such requests; to provide for exemptions; to provide for responsibilities of processors and controllers; to provide for notice and disclosure; to provide for security practices to protect consumer personal data; to allow a controller to offer different goods or services under certain conditions; to provide for limitations; to provide for enforcement and penalties; to provide an affirmative defense; to prohibit the disclosure of personal data of consumers to local governments unless pursuant to a subpoena or court order; to provide for preemption of local regulation; to provide for related matters; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, is amended by adding a new article to Chapter 1, relating to selling and other trade practices, to read as follows:

"ARTICLE 37

10-1-960.

This article shall be known and may be cited as the 'Georgia Consumer Privacy Protection Act.'

10-1-961.

As used in this article, the term:

(1) '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 purposes of this paragraph, the term 'control' or 'controlled' means:

(A) Ownership of, or the power to vote, more than 50 percent of the outstanding shares of a class of voting security of an entity;

(B) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions relative to an entity; or

(C) The power to exercise controlling influence over the management of an entity.

(2) 'Authenticate' means to verify using reasonable means that a consumer who is entitled to exercise the rights in Code Section 10-1-963, is the same consumer who is exercising such consumer rights with respect to the personal information at issue.

(3)(A) 'Biometric data' means data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris,

or other unique biological patterns or characteristics that are used to identify a specific individual.

(B) Such term shall not include:

(i) A physical or digital photograph, video recording, or audio recording or data generated from a photograph or video or audio recording; or

(ii) Information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA.

(4) 'Business associate' shall have the same meaning as provided by HIPAA.

(5) 'Consent' means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer. Such term may include a written statement, including a statement written by electronic means, or an unambiguous affirmative action.

(6) 'Consumer' means an individual who is a resident of this state acting only in a personal context. Such term shall not include an individual acting in a commercial or employment context.

(7) 'Controller' means the person that, alone or jointly with others, determines the purpose and means of processing personal information.

(8) 'Covered entity' shall have the same meaning as provided by HIPAA.

(9) 'Decisions that produce legal or similarly significant effects concerning the consumer' means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to basic necessities, such as food and water;

(10) 'De-identified data' means data that cannot reasonably be linked to an identified or identifiable individual, or any device linked to such natural person;

(11) 'Health record' means a written, printed, or electronically recorded material that:

(A) In the course of providing healthcare services to an individual was created or is maintained by a healthcare facility described in or licensed pursuant to Title 31; and

(B) Concerns the individual and the healthcare services provided.

Such term includes the substance of a communication made by an individual to a healthcare facility described in or licensed pursuant to Title 31 in confidence during or in connection with the provision of healthcare services or information otherwise acquired by the healthcare entity about an individual in confidence and in connection with the provision of healthcare services to the individual.

(12) 'HIPAA' means the federal Health Insurance Portability and Accountability Act of 1996, as amended, 42 U.S.C. Section 1320d et seq.

(13) 'Identified or identifiable individual' means a natural person who can be readily identified, whether directly or indirectly.

(14) 'Institution of higher education' means a public or private college or university in this state;

(15) 'Known child' means an individual who is under 13 years of age.

(16) 'NIST' means the National Institute of Standards and Technology privacy framework entitled 'A Tool for Improving Privacy through Enterprise Risk Management Version 1.0.'

(17) 'Nonprofit organization' means:

(A) A corporation organized under Chapter 3 of Title 14, the 'Georgia Nonprofit Corporation Code';

(B) An organization exempt from taxation under the Internal Revenue Code, codified in 26 U.S.C. Sections 501-530;

(C) A public utility organized under the laws of this state; or

(D) An entity owned or controlled by a nonprofit organization.

(18) 'Person' means any individual or entity.

(19)(A) 'Personal information' means information that is linked or reasonably linkable to an identified or identifiable individual.

(B) Such term shall not include information that:

(i) Is publicly available information;

(ii) Does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used alone or in combination with other information to identify an individual; or

(iii) Is de-identified using a method no less secure than methods provided under HIPPA.

(20)(A) '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.

(B) Such term shall not include:

(i) The content of communications; or

(ii) Data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(21) 'Process' or 'processing' means an operation or set of operations performed, whether by manual or automated means, on personal information or on sets of personal information, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal information.

(22) 'Processor' means a person that processes personal information on behalf of a controller.

(23) 'Profiling' means a form of automated processing performed on personal information solely to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(24) 'Protected health information' shall have the same meaning as provided by HIPAA.

(25) 'Pseudonymous data' means personal information that cannot be attributed to a specific individual without the use of additional information, so long as the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable individual.

(26) '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 which the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(27)(A) 'Sale of personal information' means the exchange of personal information for monetary or other valuable consideration by the controller to a third party.

(B) Such term shall not include:

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

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

(iii) The disclosure or transfer of personal information to an affiliate of the controller;

(iv) 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

(v) The disclosure or transfer of personal information 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.

(28) 'Sensitive data' means a category of personal information that includes:

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

(B) The processing of genetic or biometric data for the purpose of uniquely identifying an individual;

(C) The personal information collected from a known child; or

(D) Precise geolocation data.

(29) 'State agency' means an agency, institution, board, bureau, commission, council, or instrumentality of the executive branch of state government of this state.

(30)(A) 'Targeted advertising' means displaying to a consumer an advertisement that is selected based on personal information obtained from such consumer's activities over time and across nonaffiliated public websites or online applications to predict the consumer's preferences or interests.

(B) Such term shall not include:

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

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

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

(iv) Personal information processed solely for measuring or reporting advertising performance, reach, or frequency.

(31) 'Third party' means a person other than the consumer, controller, processor, or an affiliate of the controller or processor.

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

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

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

10-1-962.

This article shall apply to a person that conducts business in this state by producing products or services targeted to consumers of this state that exceeds $25 million in revenue and that:

(1) Controls or processes personal information of at least 25,000 consumers and derives more than 50 percent of gross revenue from the sale of personal information; or

(2) During a calendar year, controls or processes personal information of at least 175,000 consumers.

10-1-963.

(a)(1) A consumer may invoke the consumer rights authorized pursuant to paragraph (2) of 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 the consumer rights authorized pursuant to paragraph (2) of this subsection on behalf of the such known child regarding processing personal information belonging to the known child.

(2) A controller shall comply with an authenticated consumer request to exercise the right to:

(A) Confirm whether a controller is processing the consumer's personal information and to access such personal information;

(B) Correct inaccuracies in the consumer's personal information, taking into account the nature of the personal information and the purposes of the processing of such consumer's personal information;

(C) Delete personal information provided by or obtained about the consumer. A controller shall not be required to delete information that it maintains or uses as aggregate or de-identified data; provided, that such data in the possession of the controller is not linked to a specific consumer. A controller that obtained personal information about a consumer from a source other than the consumer shall be in compliance with a consumer's request to delete such personal information by retaining a record of the deletion request and the minimum information necessary for the purpose of ensuring that the consumer's personal information remains deleted from the controller's records and by not using such retained personal information for any purpose prohibited under this article;

(D) Obtain a copy of the consumer's personal information 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 such personal information to another controller without hindrance, where the processing is carried out by automated means; or

(E) Opt out of a controller's processing of personal information for purposes of:

(i) Selling personal information about the consumer;

(ii) Targeted advertising; or

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

(b) Except as otherwise provided in this article, a controller shall comply with an authenticated request by a consumer to exercise the consumer rights authorized pursuant to paragraph (2) of subsection (a) of this Code section as follows:

(1) A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of a request submitted pursuant to subsection (a) of this Code section. 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 the 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, then the controller shall inform the consumer without undue delay, but in all cases 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 subsection (c) of this Code section;

(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, technically infeasible, excessive, or repetitive, then 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, technically infeasible, excessive, or repetitive nature of the request; and

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, then the controller shall not be required to comply with a request to initiate an action under subsection (a) of this Code 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 paragraph (2) of subsection (b) of this Code section. The appeal process shall be:

(1) Made available to the consumer in a conspicuous manner;

(2) Available at no cost to the consumer; and

(3) Similar to the process for submitting requests to initiate action pursuant to subsection (a) of this Code section.

Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decision. If the appeal is denied, the controller shall then 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.

10-1-964.

(a) A controller shall:

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

(2) Except as otherwise provided in this article, not process personal information for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes for which the personal information 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, as described in Code Section 10-1-973, to protect the confidentiality, integrity, and accessibility of personal information. The data security practices shall be appropriate to the volume and nature of the personal information at issue;

(4) Not be required to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer;

(5) Not process personal information in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising the consumer rights contained in this article, 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, this paragraph shall not require a controller to provide a product or service that requires the personal information of a consumer that the controller does not collect or maintain, or 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 the right to opt out pursuant to subparagraph (E) of paragraph (2) of subsection (a) of Code Section 10-1-963 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

(6) 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 the data in accordance with the federal Children's Online Privacy Protection Act, as amended, 15 U.S.C. Section 6501 et seq., and its implementing regulations.

(b) A provision of a contract or agreement that purports to waive or limit the consumer rights described in Code Section 10-1-963 is contrary to public policy and is void and unenforceable.

(c) A controller shall provide a reasonably accessible, clear, and meaningful privacy notice that includes:

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

(2) The purpose for processing personal information;

(3) How consumers may exercise their consumer rights pursuant to Code Section 9-1-963, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) The categories of personal information that the controller sells to third parties, if any; and

(5) The categories of third parties, if any, to whom the controller sells personal information.

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

(e)(1) A controller shall provide, and shall describe in a privacy notice, one or more secure and reliable means for a consumer to submit a request to exercise the consumer rights described in Code Section 10-1-963. Such means shall take into account the:

(A) Ways in which a consumer normally interacts with the controller;

(B) Need for secure and reliable communication of such requests; and

(C) Ability of a controller to authenticate the identity of the consumer making the request.

(2) A controller shall not require a consumer to create a new account in order to exercise the consumer rights described in Code Section 10-1-963, but may require a consumer to use an existing account.

10-1-965.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this article. The assistance provided by the processor 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 reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to Code Section 10-1-963; and

(2) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to Code Section 10-1-966.

(b) A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and shall 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 information is subject to a duty of confidentiality with respect to the data;

(2) At the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information 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 article;

(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 article using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of each assessment to the controller upon request; and

(5) Engage a subcontractor pursuant to a written contract in that requires the subcontractor to meet the obligations of the processor with respect to the personal information.

(c) Nothing in this Code section shall relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as described in subsection (b) of this Code section.

(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 information is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

10-1-966.

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

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

(2) The sale of personal information;

(3) The processing of personal information for purposes of profiling, where the 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 the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

(5) Processing activities involving personal information that present a heightened risk of harm to consumers.

(b) Data protection assessments conducted pursuant to subsection (a) of this Code section 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 the processing, as mitigated by safeguards that can be employed by the controller to reduce the 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 information will be processed, shall be factored into this assessment by the controller.

(c) The Attorney General may request pursuant to a civil investigative demand that a controller disclose a 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 shall evaluate the data protection assessment for compliance with the responsibilities set forth in Code Section 10-1-964. 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 information contained in the assessment. Such data protection assessments shall be confidential and shall not be open to public inspection and copying under Article 4 of Chapter 18 of Title 50, relating to open records.

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

(e) A data protection assessment conducted by a controller for the purpose of compliance with other laws, rules, or regulations may comply with this Code section if such data protection assessment have a reasonably comparable scope and effect.

(f) The data protection assessment requirements in this article shall apply only to processing activities created or generated on or after July 1, 2024.

10-1-967.

(a) A 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 reidentify the data; and

(3) Contractually obligate recipients of the de-identified data to comply with this article.

(b) Nothing in this Code section shall require a controller or processor to:

(1) Reidentify de-identified data or pseudonymous data;

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

(3) Comply with an authenticated consumer rights request, pursuant to Code Section 10-1-963, if:

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

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

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

(c) The consumer rights described in Code Sections 10-1-963 and 10-1-964 shall not apply to pseudonymous data in cases where the controller is able to demonstrate information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing that information.

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

10-1-968.

(a) Nothing in this article shall 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 or the parent or legal guardian of a known child, 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 activity, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action;

(8) Engage in public reviewed 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 entity that determines whether:

(A) 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) The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification; or

(9) Assist another controller, processor, or third party with the obligations under this article.

(b) The obligations imposed on controllers or processors under this article 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 article shall not apply where compliance with this article by the controller or processor would violate an

evidentiary privilege under the laws of this state. Nothing in this article shall prevent a controller or processor from providing personal information concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(d)(1) A controller or processor that discloses personal information to a third-party controller or processor, in compliance with the requirements of this article, shall not be in violation of this article if:

(A) The third-party controller or processor that receives and processes the personal information is in violation of this article; and

(B) At the time of disclosing the personal information, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal information from a controller or processor in compliance with the requirements of this article is likewise not in violation of this article for the violations of the controller or processor from which it receives such personal information.

(e) This article shall not impose an obligation on controllers and processors that adversely affects the rights or freedoms of a person, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or that applies to the processing of personal information by a person in the course of a purely personal activity.

(f) A controller shall not process personal information for purposes other than those expressly listed in this Code section unless otherwise allowed by this article. Personal information processed by a controller pursuant to this Code section may be processed to the extent that the 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 information collected, used, or retained pursuant

to subsection (b) of this Code section shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention. The data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal information and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal information.

(g) If a controller processes personal information pursuant to an exemption in this Code section, then the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with subsection (f) of this Code section.

(h) Processing personal information for the purposes expressly identified in any of the paragraphs (1) through (9) of subsection of (a) of this Code Section shall not solely make an entity a controller with respect to the processing.

10-1-969.

If the Attorney General has reasonable cause to believe that an individual, controller, or processor has engaged in, is engaging in, or is about to engage in a violation of this article, then the Attorney General may issue a civil investigative demand.

10-1-970.

(a) This article shall not apply to:

(1) Any state agency, the judicial branch, the legislative branch, or any local government of this state;

(2) A financial institution, an affiliate of a financial institution, or data subject to Title V of the federal Gramm-Leach-Bliley Act, as amended, 15 U.S.C. Section 6801 et seq.;

(3) A person that is licensed in this state under Title 33 as an insurance company and transacts insurance business;

(4) A 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 federal Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);

(5) A nonprofit organization;

(6) An institution of higher education;

(7) Protected health information under HIPAA;

(8) Health records for purposes of Title 31;

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

(10) Personal information that is:

(A) Processed for purposes of:

(i) Research conducted in accordance with the federal policy for the protection of human subjects under 45 C.F.R. Part 46;

(ii) Human subjects research conducted in accordance with good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; or

(iii) Research conducted in accordance with the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56; or

(B) Processed or sold in connection with research conducted in accordance with the requirements set forth in this article, or other research conducted in accordance with applicable law;

(11) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, as amended, 42 U.S.C. Section 11101 et seq.;

(12) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, as amended, 42 U.S.C. Section 299b-21 et seq.;

(13) Information that is:

(A) Derived from the healthcare related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; or

(B) Included in a limited data set as described in 45 C.F.R. 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified in 45 C.F.R. 164.514(e);

(14) 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. Section 290dd-2;

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

(16) The collection, maintenance, disclosure, sale, communication, or use of 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 or furnisher 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, as amended, 15 U.S.C. Section 1681 et seq.;

(17) Personal information collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, as amended, 18 U.S.C. Section 2721 et seq.;

(18) Personal information or educational information regulated by the federal Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. Section 1232g et seq.;

(19) Personal information collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act, as amended, 12 U.S.C. Section 2001 et seq.;

(20) Data processed or maintained:

(A) In the course of an individual applying to, being 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 article used for emergency contact purposes; or

(C) That is necessary to retain to administer benefits for another individual relating to the individual under subparagraph (A) of this paragraph and used for the purposes of administering those benefits;

(21) Information collected as part of public reviewed or peer reviewed scientific or statistical research in the public interest;

(22) An insurance producer licensed under Title 33; or

(23) Personal information maintained or used for purposes of compliance with the regulation of listed chemicals under the federal Controlled Substances Act, as amended, 21 U.S.C. Section 830.

(b) Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act, as amended, 15 U.S.C. Section 6501 et seq., are deemed compliant with an obligation to obtain parental consent under this article.

(c) Nothing in this article shall require a controller, processor, third party, or consumer to disclose trade secrets.

10-1-971.

(a) A provision of a contract or agreement that waives or limits a consumer's rights under this article, including, but not limited to, a right to a remedy or means of enforcement, is contrary to public policy, void, and unenforceable.

(b) Nothing in this article shall prevent a consumer from declining to request information from a controller, declining to opt out of a controller's sale of the consumer's personal information, or authorizing a controller to sell the consumer's personal information after previously opting out.

(c) This article shall apply to contracts entered into, amended, or renewed on or after July 1, 2024.

10-1-972.

(a) The Attorney General has exclusive authority to enforce this article.

(b) The Attorney General may develop reasonable cause to believe that a controller or processor is in violation of this article, based on the Attorney General's own inquiry or on consumer or public complaints. Prior to initiating an action under this article, the Attorney General shall provide a controller or processor 60 days' written notice identifying the specific provisions of this article the Attorney General alleges have been or are being violated. If within the 60 day period, 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 such further violations shall occur, then the Attorney General shall not initiate an action against the controller or processor.

(c) If a controller or processor continues to violate this article following the cure period provided for in subsection (b) of this Code section or breaches an express written statement provided to the Attorney General under subsection (b) of this Code section, then the Attorney General may bring an action in a court of competent jurisdiction seeking any of the following relief:

(1) Declaratory judgment that the act or practice violates this article;

(2) Injunctive relief, including preliminary and permanent injunctions, to prevent an additional violation of and compel compliance with this article;

(3) Civil penalties, as described in subsection (d) of this Code section;

(4) Reasonable attorney's fees and investigative costs; or

(5) Other relief the court determines appropriate.

(d)(1) A court may impose a civil penalty of up to $7,500.00 for each violation of this article.

(2) If the court finds the controller or processor willfully or knowingly violated this article, then the court may, in its discretion, award treble damages.

(e) A violation of this article shall not serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under this article or any other law.

(f) The Attorney General may recover reasonable expenses incurred in investigating and preparing a case, including attorney's fees, in an action initiated under this article.

10-1-973.

(a) A controller or processor shall have an affirmative defense to a cause of action for a violation of this article if the controller or processor creates, maintains, and complies with a written privacy policy that:

(1)(A) Reasonably conforms to the NIST or other documented policies, standards, and procedures designed to safeguard consumer privacy; and

(B) Is updated to reasonably conform with a subsequent revision to the NIST or comparable privacy framework within two years of the publication date stated in the most recent revision to the NIST or comparable privacy framework; and

(2) Provides a person with the substantive rights required by this article.

(b) The scale and scope of a controller or processor's privacy program under subsection (a) of this Code section shall be appropriate if it is based on all of the following factors:

(1) The size and complexity of the controller or processor's business;

(2) The nature and scope of the activities of the controller or processor;

(3) The sensitivity of the personal information processed;

(4) The cost and availability of tools to improve privacy protections and data governance; and

(5) Compliance with a comparable state or federal law.

10-1-974.

(a) No municipality, county, or consolidated government shall not require a controller or processor to disclose personal data of consumers, unless pursuant to a subpoena or court order.

(b) This article shall supersede and preempt any conflicting provisions of any ordinances, resolutions, regulations, or the equivalent adopted by any municipality, county, or consolidated government regarding the processing of personal data by controllers or processors."

SECTION 2.

All laws and parts of laws in conflict with this Act are repealed.