Sen. Sue Rezin

Filed: 3/13/2025

AMENDMENT TO SENATE BILL 51

AMENDMENT NO. _____. Amend Senate Bill 51 by replacing everything after the enacting clause with the following:

"Section 1. Short title. This Act may be cited as the Illinois Consumer Data Privacy Act.

Section 5. Definitions. As used in this Act:

"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% 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 consumer rights granted in Section 15 is the same consumer exercising 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 are 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, unless that data is generated to identify a specific individual or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

"Business associate" has the same meaning as in 45 CFR Sec. 160.103 under HIPAA.

"Child" has the same meaning as in 15 U.S.C. Sec. 6501.

"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" includes a written statement, written by electronic means, or any other unambiguous affirmative action.

"Consumer" means a natural person who is a resident of the

State acting only in an individual context. "Consumer" does not include a natural person acting in a commercial or employment context.

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

"Covered entity" has the same meaning as in 45 CFR Sec. 160.103 under HIPAA.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by a 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 like food and water.

"Deidentified data" means data that cannot reasonably be linked to an identified or identifiable natural person or a device linked to a person.

"Fund" means the Consumer Privacy Fund established in Section 50.

"Health record" means a record, other than for financial or billing purposes, relating to an individual, kept by a health care provider as a result of the professional relationship established between the health care provider and the individual.

"Health care provider" means:

(1) any health care facility as defined in Section 8-2001 of the Code of Civil Procedure;

(2) health care practitioner as defined in Section 8-2001 of the Code of Civil Procedure;

(3) the current and former employers, officers, directors, administrators, agents, or employees of those entities listed in paragraphs (1) and (2); or

(4) any person acting within the course and scope of the office, employment, or agency relating to a health care facility or a health care practitioner.

"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996.

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

"Institution of higher education" means an educational institution that:

(1) admits as regular students only individuals having a certificate of graduation from a high school, or the recognized equivalent of such a certificate;

(2) is legally authorized in this State to provide a program of education beyond high school;

(3) provides an educational program for which it awards a bachelor's or higher degree, or provides a program that is acceptable for full credit toward such a degree, a program of postgraduate or postdoctoral studies, or a program of training to prepare students for gainful

employment in a recognized occupation; and

(4) is a public or other nonprofit institution.

"Nonprofit organization" means any incorporated or unincorporated entity that:

(1) is operating for religious, charitable, or educational purposes; and

(2) does not provide net earnings to, or operate in any manner that inures to the benefit of, any officer, employee, or shareholder of the entity.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified 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, including, but not limited to, 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" has the same meaning as in 45 CFR Sec. 160.103 under HIPAA.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, as long as the 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 monetary consideration by the controller to a 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 intentionally made available to the general public via a channel of mass media and 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 proposed or actual 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 indicating 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 that

is processed for the purpose of uniquely identifying a specific natural person;

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

(4) precise geolocation data.

"State agency" means:

(1) all departments, offices, commissions, boards, institutions, and political and corporate bodies of the State;

(2) the Supreme Court, appellate courts, and circuit courts; and

(3) the General Assembly, its committees, or commissions.

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

(1) advertisements based on activities within a controller's own or affiliated 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 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" has the same meaning as in the Illinois Trade Secrets Act.

Section 10. Coverage of act.

(a) This Act applies to persons that conduct business in the State or produce products or services that are targeted to State residents and that during a calendar year control or process personal data of at least:

(1) 100,000 consumers; or

(2) 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.

(b) This Act does not apply to any:

(1) unit of local government, State, or any political subdivision of the State;

(2) financial institution, its affiliate, or data subject to Title V of the federal Gramm-Leach-Bliley Act;

(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 CFR Parts 160 and 164 established under

HIPAA;

(4) nonprofit organization;

(5) institution of higher education;

(6) law enforcement agency in connection with suspected insurance-related criminal or fraudulent acts or first responders in connection with catastrophic events; or

(7) public utility as defined in the Public Utilities Act;

(c) The following information and data are exempt from this Act:

(1) protected health information under HIPAA;

(2) health records;

(3) patient identifying information for purposes of 42 CFR Sec. 2.11;

(4) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR Part 46; identifiable private information that is otherwise information collected as part of human subjects research under 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 CFR Parts 50 and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this Act, 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;

(6) patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act;

(7) information derived from any of the health care-related information listed in this subsection that is deidentified in accordance with the requirements for deidentification under HIPAA;

(8) information originating from, and intermingled to be indistinguishable from, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate, or a program or qualified service organization as defined by 42 3 CFR Sec. 2.11;

(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 creditworthiness, 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 the activity is regulated by and authorized under the federal Fair Credit

Reporting Act;

(11) personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

(12) personal data regulated by the federal Family Educational Rights and Privacy Act;

(13) personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act;

(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 used for emergency contact purposes; or

(C) that is necessary to administer benefits for another individual and used for the purposes of administering those benefits;

(15) data processed by a public utility, an affiliate of a public utility, or a holding company system organized specifically for the purpose of providing goods or services to a public utility. For purposes of this paragraph, "holding company system" means 2 or more affiliated persons, one or more of which is a public utility; and

(16) personal data collected and used for purposes of federal policy under the Combat Methamphetamine Epidemic Act of 2005.

(d) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act are deemed compliant with any obligation to obtain parental consent under this Act.

Section 15. Consumer rights and remedies.

(a) A consumer may invoke the consumer rights authorized under this Section at any time by submitting a request to a controller, via the means specified by the controller under Section 20, specifying the consumer rights the consumer wishes to invoke. A child's parent or legal guardian may invoke these consumer rights on behalf of the child regarding processing personal data belonging to the child.

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

(1) confirm whether a controller is processing the consumer's personal data and to access the personal data, unless the confirmation and access would require the controller to reveal a trade secret;

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

(3) delete personal data provided by or obtained about

the consumer;

(4) 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 practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, if the processing is carried out by automated means. The controller may not be required to reveal any trade secrets; and

(5) opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(c) Except as otherwise provided in this Act, a controller shall comply with a request by a consumer to exercise the consumer rights under this Section 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 under the methods described in this Section. The response period may be extended once by 45 additional days if reasonably necessary, taking into consideration the complexity and number of the consumer's requests, as long as the controller informs the consumer of any 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 no later than 45 days after receipt of the request of the justification for declining to take action and instructions on how to appeal that decision;

(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 excessive, repetitive, technically infeasible, or manifestly unfounded, 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 excessive, repetitive, technically infeasible, or manifestly unfounded nature of the request;

(4) if a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a request to initiate an action under this Section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request; and

(5) a controller that has obtained personal data about a consumer from a source other than the consumer is deemed

in compliance with a consumer's request to delete such data under this Section by:

(A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business' records and not using the retained data for any other purpose under the provisions of this Act; or

(B) opting the consumer out of the processing of the personal data for any other purpose unless authorized elsewhere in this Act.

(d) 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 under of this Section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action under this Section. 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.

Section 20. Controller's duties and responsibilities.

(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 the data is processed as disclosed to the consumer;

(2) except as otherwise provided in this Section, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the 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. The 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 this Act, 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. Nothing in this paragraph may 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 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 collected from a known child, process the data in accordance with the federal Children's Online Privacy Protection Act.

(b) Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights under this Act is deemed contrary to public policy and is 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 under this Act, including how a consumer may appeal a

controller's decision regarding a 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 activity, as well as the manner in which a consumer may exercise the right to opt out of 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 Act. The different ways to submit a request by a consumer must consider the ways in which consumers normally interact with the controller, the need for secure and reliable communication of the requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers may not require a consumer to create a new account to exercise consumer rights under this Act but may require a consumer to use an existing account.

Section 25. Processor duties and responsibilities.

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

(1) supporting the controller's obligation to respond to consumer rights requests under this Act by taking into account the nature of processing and the information available to the processor using appropriate technical and organizational measures as reasonably practicable;

(2) assisting the controller in meeting the controller's obligations for the security of processing the personal data and for the notification of a breach of the security of the system of the processor under applicable State law by taking into account the nature of processing and the information available to the processor; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments under this Act.

(b) A contract between a controller and a processor governs the processor's data processing procedures for processing performed on behalf of the controller. The contract shall be binding and shall clearly set forth instructions for processing personal 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 Act;

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

(5) engage any subcontractor under a written contract under this Section that requires the subcontractor to meet the obligations of the processor for personal data.

(c) Nothing in this Section may be construed to relieve a controller or processor from the liabilities imposed on it by virtue of its role in a processing relationship as required under this Act.

(d) Determining whether a person is acting as a controller or processor for 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 for a specific processing of personal data remains a processor.

Section 30. Required data protection impact assessment.

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

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

(2) the processing of personal data for the purposes of selling of personal data;

(3) the processing of personal data for the purposes of profiling, if the profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of consumers or disparate impact on consumers;

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

(C) a physical or other intrusion upon consumers' solitude or seclusion or their private affairs or concerns if an 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 of personal data that presents a heightened risk of harm to consumers.

(b) Data protection impact assessments conducted under this 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 such processing, as mitigated by safeguards that can be employed by the controller to reduce the risk. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing of personal data 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 that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection impact assessment available to the Attorney General. The Attorney General may evaluate the data protection impact assessments for compliance with the requirements of this Act.

(d) Data protection impact assessments are confidential and exempt from disclosure, public inspection, and copying under the Freedom of Information Act.

(e) The disclosure of a data protection impact assessment under a request from the Attorney General under this Section does not constitute a waiver of the attorney-client privilege or work product protection of the assessment and any information contained in the assessment.

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

(g) 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.

(h) Data protection assessment requirements apply to processing activities created or generated on or after June 1, 2027.

Section 35. Controller in possession of de-identified data.

(a) The controller in possession of deidentified data shall:

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

(2) publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and

(3) contractually obligate any recipients of the

deidentified data to comply with this Act.

(b) Nothing in this Act may be construed to require a controller or processor to:

(1) reidentify deidentified data or pseudonymous data; or

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

(c) Nothing in this Act may be construed to require a controller or processor to comply with an authenticated consumer rights request under Section 15 if:

(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 this Act do not apply

to pseudonymous data in cases in which the controller is able to demonstrate any information necessary to identify the consumer 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.

(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 deidentified data is subject and take appropriate steps to address any breaches of those contractual commitments.

Section 40. Exceptions for controllers and processors.

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

(1) comply with federal, State, or local laws 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 a parent or guardian of a known child;

(6) perform a contract to which the consumer or parent or guardian of a known child is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of the consumer or parent or guardian of a known child before entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person;

(9) 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;

(10) 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

(11) assist another controller, processor, or third party with any of the obligations under this Section.

(b) The obligations imposed on controllers or processors under this Act do 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 a parent or guardian of a known child or the performance of a contract to which the consumer or a

parent or guardian of a known child is a party.

(c) The obligations imposed on controllers or processors under this Act do not apply to a controller or processor if compliance would violate an evidentiary privilege under State law. Nothing in this Act may be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under State laws 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 Act, is not in violation of this Act if the third-party controller or processor that receives and processes such personal data is in violation of this Act; 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 Act is also not in violation of this Act for the transgressions of the controller or processor from which it receives such personal data.

(e) Nothing in this Act may be construed as an obligation imposed on controllers and processors that adversely affects the privacy or other rights or freedoms of any persons, including, but not limited to, the right of free speech under

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 under this Section may not be processed for any purpose other than those expressly listed unless otherwise allowed by this Act. Personal data processed by a controller under 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 for the specific purposes listed in this Section. Personal data collected, used, or retained under this Section shall, if applicable, take into account the nature and purpose or purposes of such collection, use, or retention. The data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(g) If a controller processes personal data under an exemption in this Section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in this Section.

(h) Processing personal data for the purposes expressly

identified in this Section does not by itself make an entity a controller with respect to such processing.

Section 45. Enforcement by the Attorney General.

(a) The Attorney General has exclusive authority to enforce violations of this Act. The Attorney General may enforce this Act by bringing an action in the name of the State of Illinois on behalf of persons residing in this State. The Attorney General has all powers and duties granted to the Attorney General under State law to investigate and prosecute any violation of this Act. The Attorney General may demand any information, documents, or physical evidence from any controller or processor believed to be engaged in, or about to engage in, any violation of this Act.

(b) Before initiating any action for a violation of this Act, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this Act that the Attorney General 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 will occur, no action for damages under this Section may be initiated against the controller or processor.

(c) If a controller or processor continues to violate this

Act following the cure period under this Section or breaches an express written statement provided to the Attorney General under this Section, the Attorney General may initiate an action and seek damages for up to $7,500 for each continued violation under this Act.

(d) Nothing in this Act or any other law, regulation, or the equivalent may be construed as providing the basis for, or give rise to, a private right of action for violations of this Act.

(e) The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, court costs, attorney's fees, and any other relief ordered by the court of any action initiated under this Act.

Section 50. Consumer Privacy Fund. This Act hereby creates the Consumer Privacy Fund. The Fund shall be administered by the Office of the Attorney General. All civil penalties collected under this Act shall be deposited into the Fund. Interest earned on moneys in the Fund accrue to the Fund. Moneys in the fund shall be used by the Office of the Attorney General to enforce this Act.

Section 900. The Freedom of Information Act is amended by changing Section 7 as follows:

(5 ILCS 140/7)

Sec. 7. Exemptions.

(1) When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:

(a) Information specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law.

(b) Private information, unless disclosure is required by another provision of this Act, a State or federal law, or a court order.

(b-5) Files, documents, and other data or databases maintained by one or more law enforcement agencies and specifically designed to provide information to one or more law enforcement agencies regarding the physical or mental status of one or more individual subjects.

(c) Personal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. "Unwarranted invasion of personal privacy" means the disclosure of

information that is highly personal or objectionable to a reasonable person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.

(d) Records in the possession of any public body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:

(i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;

(ii) interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;

(iii) create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;

(iv) unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to

administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic crashes, traffic crash reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;

(v) disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation, or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;

(vi) endanger the life or physical safety of law enforcement personnel or any other person; or

(vii) obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

(d-5) A law enforcement record created for law enforcement purposes and contained in a shared electronic record management system if the law enforcement agency that is the recipient of the request did not create the record, did not participate in or have a role in any of the events which are the subject of the record, and only has

access to the record through the shared electronic record management system.

(d-6) Records contained in the Officer Professional Conduct Database under Section 9.2 of the Illinois Police Training Act, except to the extent authorized under that Section. This includes the documents supplied to the Illinois Law Enforcement Training Standards Board from the Illinois State Police and Illinois State Police Merit Board.

(d-7) Information gathered or records created from the use of automatic license plate readers in connection with Section 2-130 of the Illinois Vehicle Code.

(e) Records that relate to or affect the security of correctional institutions and detention facilities.

(e-5) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials are available in the library of the correctional institution or facility or jail where the inmate is confined.

(e-6) Records requested by persons committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail if those materials include records from staff members' personnel files, staff rosters, or other staffing assignment information.

(e-7) Records requested by persons committed to the Department of Corrections or Department of Human Services Division of Mental Health if those materials are available through an administrative request to the Department of Corrections or Department of Human Services Division of Mental Health.

(e-8) Records requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, the disclosure of which would result in the risk of harm to any person or the risk of an escape from a jail or correctional institution or facility.

(e-9) Records requested by a person in a county jail or committed to the Department of Corrections or Department of Human Services Division of Mental Health, containing personal information pertaining to the person's victim or the victim's family, including, but not limited to, a victim's home address, home telephone number, work or school address, work telephone number, social security number, or any other identifying information, except as may be relevant to a requester's current or potential case or claim.

(e-10) Law enforcement records of other persons requested by a person committed to the Department of Corrections, Department of Human Services Division of Mental Health, or a county jail, including, but not

limited to, arrest and booking records, mug shots, and crime scene photographs, except as these records may be relevant to the requester's current or potential case or claim.

(f) Preliminary drafts, notes, recommendations, memoranda, and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body. The exemption provided in this paragraph (f) extends to all those records of officers and agencies of the General Assembly that pertain to the preparation of legislative documents.

(g) Trade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged, or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.

The information included under this exemption includes all trade secrets and commercial or financial information obtained by a public body, including a public pension fund, from a private equity fund or a privately held

company within the investment portfolio of a private equity fund as a result of either investing or evaluating a potential investment of public funds in a private equity fund. The exemption contained in this item does not apply to the aggregate financial performance information of a private equity fund, nor to the identity of the fund's managers or general partners. The exemption contained in this item does not apply to the identity of a privately held company within the investment portfolio of a private equity fund, unless the disclosure of the identity of a privately held company may cause competitive harm.

Nothing contained in this paragraph (g) shall be construed to prevent a person or business from consenting to disclosure.

(h) Proposals and bids for any contract, grant, or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person proposing to enter into a contractor agreement with the body, until an award or final selection is made. Information prepared by or for the body in preparation of a bid solicitation shall be exempt until an award or final selection is made.

(i) Valuable formulae, computer geographic systems, designs, drawings, and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. The

exemption for "computer geographic systems" provided in this paragraph (i) does not extend to requests made by news media as defined in Section 2 of this Act when the requested information is not otherwise exempt and the only purpose of the request is to access and disseminate information regarding the health, safety, welfare, or legal rights of the general public.

(j) The following information pertaining to educational matters:

(i) test questions, scoring keys, and other examination data used to administer an academic examination;

(ii) information received by a primary or secondary school, college, or university under its procedures for the evaluation of faculty members by their academic peers;

(iii) information concerning a school or university's adjudication of student disciplinary cases, but only to the extent that disclosure would unavoidably reveal the identity of the student; and

(iv) course materials or research materials used by faculty members.

(k) Architects' plans, engineers' technical submissions, and other construction related technical documents for projects not constructed or developed in whole or in part with public funds and the same for

projects constructed or developed with public funds, including, but not limited to, power generating and distribution stations and other transmission and distribution facilities, water treatment facilities, airport facilities, sport stadiums, convention centers, and all government owned, operated, or occupied buildings, but only to the extent that disclosure would compromise security.

(l) Minutes of meetings of public bodies closed to the public as provided in the Open Meetings Act until the public body makes the minutes available to the public under Section 2.06 of the Open Meetings Act.

(m) Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil, or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies.

(n) Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption shall not extend to the final outcome of cases in which discipline is imposed.

(o) Administrative or technical information associated with automated data processing operations, including, but

not limited to, software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

(p) Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.

(q) Test questions, scoring keys, and other examination data used to determine the qualifications of an applicant for a license or employment.

(r) The records, documents, and information relating to real estate purchase negotiations until those negotiations have been completed or otherwise terminated. With regard to a parcel involved in a pending or actually and reasonably contemplated eminent domain proceeding under the Eminent Domain Act, records, documents, and information relating to that parcel shall be exempt except as may be allowed under discovery rules adopted by the Illinois Supreme Court. The records, documents, and information relating to a real estate sale shall be exempt until a sale is consummated.

(s) Any and all proprietary information and records related to the operation of an intergovernmental risk management association or self-insurance pool or jointly self-administered health and accident cooperative or pool. Insurance or self-insurance (including any intergovernmental risk management association or self-insurance pool) claims, loss or risk management information, records, data, advice, or communications.

(t) Information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of a public body responsible for the regulation or supervision of financial institutions, insurance companies, or pharmacy benefit managers, unless disclosure is otherwise required by State law.

(u) Information that would disclose or might lead to the disclosure of secret or confidential information, codes, algorithms, programs, or private keys intended to be used to create electronic signatures under the Uniform Electronic Transactions Act.

(v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, but only to the extent that disclosure could reasonably be expected to expose the vulnerability

or jeopardize the effectiveness of the measures, policies, or plans, or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, to cybersecurity vulnerabilities, or to tactical operations.

(w) (Blank).

(x) Maps and other records regarding the location or security of generation, transmission, distribution, storage, gathering, treatment, or switching facilities owned by a utility, by a power generator, or by the Illinois Power Agency.

(y) Information contained in or related to proposals, bids, or negotiations related to electric power procurement under Section 1-75 of the Illinois Power Agency Act and Section 16-111.5 of the Public Utilities Act that is determined to be confidential and proprietary by the Illinois Power Agency or by the Illinois Commerce Commission.

(z) Information about students exempted from disclosure under Section 10-20.38 or 34-18.29 of the School Code, and information about undergraduate students enrolled at an institution of higher education exempted from disclosure under Section 25 of the Illinois Credit Card Marketing Act of 2009.

(aa) Information the disclosure of which is exempted under the Viatical Settlements Act of 2009.

(bb) Records and information provided to a mortality review team and records maintained by a mortality review team appointed under the Department of Juvenile Justice Mortality Review Team Act.

(cc) Information regarding interments, entombments, or inurnments of human remains that are submitted to the Cemetery Oversight Database under the Cemetery Care Act or the Cemetery Oversight Act, whichever is applicable.

(dd) Correspondence and records (i) that may not be disclosed under Section 11-9 of the Illinois Public Aid Code or (ii) that pertain to appeals under Section 11-8 of the Illinois Public Aid Code.

(ee) The names, addresses, or other personal information of persons who are minors and are also participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations.

(ff) The names, addresses, or other personal information of participants and registrants in programs of park districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations where such programs are targeted primarily to minors.

(gg) Confidential information described in Section 1-100 of the Illinois Independent Tax Tribunal Act of 2012.

(hh) The report submitted to the State Board of Education by the School Security and Standards Task Force under item (8) of subsection (d) of Section 2-3.160 of the School Code and any information contained in that report.

(ii) Records requested by persons committed to or detained by the Department of Human Services under the Sexually Violent Persons Commitment Act or committed to the Department of Corrections under the Sexually Dangerous Persons Act if those materials: (i) are available in the library of the facility where the individual is confined; (ii) include records from staff members' personnel files, staff rosters, or other staffing assignment information; or (iii) are available through an administrative request to the Department of Human Services or the Department of Corrections.

(jj) Confidential information described in Section 5-535 of the Civil Administrative Code of Illinois.

(kk) The public body's credit card numbers, debit card numbers, bank account numbers, Federal Employer Identification Number, security code numbers, passwords, and similar account information, the disclosure of which could result in identity theft or impression or defrauding of a governmental entity or a person.

(ll) Records concerning the work of the threat assessment team of a school district, including, but not limited to, any threat assessment procedure under the School Safety Drill Act and any information contained in the procedure.

(mm) Information prohibited from being disclosed under subsections (a) and (b) of Section 15 of the Student Confidential Reporting Act.

(nn) Proprietary information submitted to the Environmental Protection Agency under the Drug Take-Back Act.

(oo) Records described in subsection (f) of Section 3-5-1 of the Unified Code of Corrections.

(pp) Any and all information regarding burials, interments, or entombments of human remains as required to be reported to the Department of Natural Resources pursuant either to the Archaeological and Paleontological Resources Protection Act or the Human Remains Protection Act.

(qq) Reports described in subsection (e) of Section 16-15 of the Abortion Care Clinical Training Program Act.

(rr) Information obtained by a certified local health department under the Access to Public Health Data Act.

(ss) For a request directed to a public body that is also a HIPAA-covered entity, all information that is protected health information, including demographic

information, that may be contained within or extracted from any record held by the public body in compliance with State and federal medical privacy laws and regulations, including, but not limited to, the Health Insurance Portability and Accountability Act and its regulations, 45 CFR Parts 160 and 164. As used in this paragraph, "HIPAA-covered entity" has the meaning given to the term "covered entity" in 45 CFR 160.103 and "protected health information" has the meaning given to that term in 45 CFR 160.103.

(tt) Proposals or bids submitted by engineering consultants in response to requests for proposal or other competitive bidding requests by the Department of Transportation or the Illinois Toll Highway Authority.

(uu) Disclosure data protection impact assessments done under the Illinois Consumer Data Privacy Act.

(1.5) Any information exempt from disclosure under the Judicial Privacy Act shall be redacted from public records prior to disclosure under this Act.

(2) A public record that is not in the possession of a public body but is in the possession of a party with whom the agency has contracted to perform a governmental function on behalf of the public body, and that directly relates to the governmental function and is not otherwise exempt under this Act, shall be considered a public record of the public body, for purposes of this Act.

(3) This Section does not authorize withholding of information or limit the availability of records to the public, except as stated in this Section or otherwise provided in this Act.

(Source: P.A. 102-38, eff. 6-25-21; 102-558, eff. 8-20-21; 102-694, eff. 1-7-22; 102-752, eff. 5-6-22; 102-753, eff. 1-1-23; 102-776, eff. 1-1-23; 102-791, eff. 5-13-22; 102-982, eff. 7-1-23; 102-1055, eff. 6-10-22; 103-154, eff. 6-30-23; 103-423, eff. 1-1-24; 103-446, eff. 8-4-23; 103-462, eff. 8-4-23; 103-540, eff. 1-1-24; 103-554, eff. 1-1-24; 103-605, eff. 7-1-24; 103-865, eff. 1-1-25.)

Section 905. The State Finance Act is amended by adding Section 5.1030 as follows:

(30 ILCS 105/5.1030 new)

Sec. 5.1030. The Consumer Privacy Fund.".