SB2875

LRB10417139JRC30558b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

SB2875

Introduced 1/16/2026, by Sen. Laura M. Murphy

SYNOPSIS AS INTRODUCED:

New Act

Creates the Illinois Consumer Data Privacy Act. Applies to legal entities that conduct business in Illinois or produce products or services that are targeted to Illinois residents and that satisfy one or more of the following thresholds: during a calendar year, controls or processes personal data of 100,000 consumers or more, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person but does not include deidentified data or publicly available information. Requires a controller who, alone or jointly with others, to consider the purposes and means of the processing of personal data in protecting the security of consumers while processing personal data and in notifying consumers of a breach of the security of the system. Authorizes rights to consumers under the Act to include, but not be limited to, the right to access their personal data, obtain a list of third parties to whom their data has been disclosed, request corrections to inaccurate data, and question the profiling of their information. Creates an appeal process for a consumer to gather more information on the actions of a covered entity. Exempts the State, a political subdivision of the State, and units of local government, a federally recognized Indian tribe, nonprofits established to prevent insurance fraud, and data already covered by federal law. Authorizes the Attorney General to enforce the Act. Makes definitions. Makes other changes. Limits the concurrent exercise of home rule powers. Contains a severability provision.

LRB104 17139 JRC 30558 b

A BILL FOR

AN ACT concerning civil law.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 10. Short title. This Act may be cited as the Illinois Consumer Data Privacy Act.

Section 11. Definitions. As used in this Act:

(a) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity. As used in this definition, "control" or "controlled" means: ownership of or the power to vote more than 50% of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(b) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights under Section 14, subsection (1), paragraphs (b) to (h), is being made by or rightfully on behalf of the consumer who is entitled to exercise the rights with respect to the personal data at issue.

(c) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics,

including a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. Biometric data does not include:

(1) a digital or physical photograph;

(2) an audio or video recording; or

(3) any data generated from a digital or physical photograph, or an audio or video recording, unless the data is generated to identify a specific individual.

(d) "Child" has the meaning given in United States Code, Title 15, Section 6501.

(e) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer. Acceptance of general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. A consent is not valid when the consumer's indication has been obtained by a dark pattern. A consumer may revoke consent previously given consistent with this Act.

(f) "Consumer" means a natural person who is an Illinois resident acting only in an individual or household context. Consumer does not include a natural person acting in a commercial or employment context.

(g) "Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

(h) "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, health care services, or access to essential goods or services.

(i) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(j) "Deidentified data" means data that cannot reasonably be used to infer information about or otherwise be linked to an identified or identifiable natural person or a device linked to an identified or identifiable natural person, provided that the controller that possesses the data:

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

(2) publicly commits to process the data only in a deidentified fashion and not attempt to reidentify the data; and

(3) contractually obligates any recipients of the information to comply with all provisions of this definition.

(k) "Delete" means to remove or destroy information so that it is not maintained in human- or machine-readable form and cannot be retrieved or used in the ordinary course of business.

(l) "Genetic information" means information about an identifiable individual derived from the presence, absence, alteration, or mutation of a gene, or the presence or absence of a specific DNA or RNA marker, which has been obtained from an analysis of:

(1) the individual's biological information or specimen; or

(2) the biological information or specimen of a person to whom the individual is related.

"Genetic information" also means medical or biological information collected from an individual about a particular genetic condition that is or might be used to provide medical care to that individual or the individual's family members.

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

(n) "Known child" means a person under circumstances in which a controller has actual knowledge of, or willfully disregards, that the person is under 13 years of age.

(o) "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. As used in this

definition, "publicly available information" means information that (1) is lawfully made available from federal, state, or local government records or widely distributed media; or (2) a controller has a reasonable basis to believe has lawfully been made available to the general public.

(p) "Process" or "processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, including, but not limited to, the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(q) "Processor" means a natural or legal person who processes personal data on behalf of a controller.

(r) "Profiling" means any form of automated processing of 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.

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

(t) "Sale", "sell", or "sold" means the exchange of personal data for monetary or other valuable consideration by

the controller to a third party. "Sale" does not include the following:

(1) the disclosure of personal data to a processor who 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;

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

(6) the exchange of personal data between the producer of a good or service and authorized agents of the producer who sell and service the goods and services to enable the cooperative provisioning of goods and services by both the producer and the producer's agents.

(u) "Sensitive data" is a form of personal data. "Sensitive data" means:

(1) personal data revealing racial or ethnic origin,

religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status;

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

(3) the personal data of a known child; or

(4) specific geolocation data.

(v) "Specific 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 geographic coordinates of a consumer or a device linked to a consumer with an accuracy of more than 3 decimal degrees of latitude and longitude or the equivalent in an alternative geographic coordinate system or a street address derived from the coordinates. Specific geolocation data does not include the content of communications, the contents of databases containing street address information that are accessible to the public as authorized by law, or any data generated by or connected to advanced utility metering infrastructure systems or other equipment for use by a public utility.

(w) "Targeted advertising" means displaying advertisements to a consumer in which the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or

online applications to predict the consumer's preferences or interests. Targeted advertising does not include:

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

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

(3) advertising 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.

"Technology provider" means a person who:

(1) contracts with a public educational agency or institution, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and

(2) creates, receives, or maintains educational data pursuant or incidental to a contract with a public educational agency or institution.

(x) "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.

(y) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) derives independent economic value, actual or

potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The existence of a trade secret is not negated merely because an employee or other person has acquired the trade secret without express or specific notice that it is a trade secret if, under all the circumstances, the employee or other person knows or has reason to know that the owner intends or expects the secrecy of the type of information comprising the trade secret to be maintained.

Section 12. Scope; exclusions.

(a)(1) Scope. This Act applies to legal entities that conduct business in Illinois or produce products or services that are targeted to Illinois residents, and that satisfy one or more of the following thresholds:

(A) during a calendar year, controls or processes personal data of 100,000 consumers or more, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(B) derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.

(2) A controller or processor shall comply with the Student Online Personal Protection Act, except that when the provisions of that Act conflict with this Act, the Consumer Data Privacy Act prevails.

(b) Exclusions. The provisions of this Act do not apply to the following entities, activities, or types of information:

(1) the State, a political subdivision of the State, and units of local government;

(2) a federally recognized Indian tribe;

(3) information that meets the definition of:

(A) protected health information, as defined by and for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(B) health records, that includes, but is not limited to, any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient;

(C) patient identifying information for purposes of Code of Federal Regulations, Title 42, Part 2, established pursuant to the United States Code, Title 42, Section 290dd-2;

(D) identifiable private information for purposes

of the federal policy for the protection of human subjects, the Code of Federal Regulations, Title 45, 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; the protection of human subjects under the Code of Federal Regulations, Title 21, Parts 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the requirements set forth in this paragraph;

(E) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, Public Law 99-660, and related regulations; or

(F) patient safety work product for purposes of Code of Federal Regulations, Title 42, Part 3, established under the United States Code, Title 42, Sections 299b-21 to 299b-26;

(4) information that is derived from any of the health care-related information listed in clause (3), but that has been deidentified in accordance with the requirements for deidentification set forth in the Code of Federal Regulations, Title 45, Part 164;

(5) information originating from, and intermingled to be indistinguishable with, any of the health care-related information listed in clause (3) that is maintained by:

(A) a covered entity or business associate, as defined by the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(B) a health care provider, to include, but not be limited to, any public or private facility that provides, on an inpatient or outpatient basis, preventive, diagnostic, therapeutic, convalescent, rehabilitation, mental health, or intellectual disability services, including general or special hospitals, skilled nursing homes, extended care facilities, intermediate care facilities and mental health centers; or

(C) a program or a qualified service organization, as defined by Code of Federal Regulations, Title 42, Part 2, established pursuant to United States Code, Title 42, Section 290dd-2;

(6) information that is:

(A) maintained by an entity that meets the definition of health care provider under the Code of Federal Regulations, Title 45, Section 160.103, to the extent that the entity maintains the information in the manner required of covered entities with respect to protected health information for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(B) included in a limited data set, as described under the Code of Federal Regulations, Title 45, Part 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by that part;

(C) maintained by, or maintained to comply with the rules or orders of, a self-regulatory organization as defined by the United States Code, Title 15, Section 78c(a)(26);

(D) originated from, or intermingled with, information described in clause (9) and that a residential mortgage originator or residential mortgage servicer regulated under the Residential Mortgage License Act of 1987 collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified in clause (9); or

(E) originated from, or intermingled with, information described in clause (9) and that a nonbank financial institution collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified in clause (9);

(7) information used only for public health activities and purposes, as described under the Code of Federal Regulations, Title 45, Part 164.512;

(8) an activity involving the collection, maintenance,

disclosure, sale, communication, or use of any personal data 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, as defined in the United States Code, Title 15, Section 1681a(f), by a furnisher of information, as set forth in the United States Code, Title 15, Section 1681s-2, who provides information for use in a consumer report, as defined in the United States Code, Title 15, Section 1681a(d), and by a user of a consumer report, as set forth in the United States Code, Title 15, Section 1681b, except that information is only excluded under this paragraph to the extent that the activity involving the collection, maintenance, disclosure, sale, communication, or use of the information by the agency, furnisher, or user is subject to regulation under the federal Fair Credit Reporting Act, United States Code, Title 15, Sections 1681 to 1681x, and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act;

(9) personal data collected, processed, sold, or disclosed under the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

(10) personal data collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, United States Code, Title 18, Sections 2721 to 2725, if the collection, processing, sale, or disclosure is in compliance with that law;

(11) personal data regulated by the federal Family Educational Rights and Privacy Act, United States Code, Title 20, Section 1232g, and implementing regulations;

(12) personal data collected, processed, sold, or disclosed pursuant to the federal Farm Credit Act of 1971, as amended, United States Code, Title 12, Sections 2001 to 2279cc, and implementing regulations, Code of Federal Regulations, Title 12, Part 600, if the collection, processing, sale, or disclosure is in compliance with that law;

(13) data collected or maintained:

(A) in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of a business if the data is collected and used solely within the context of the role;

(B) as the emergency contact information of an individual under item (1) if used solely for emergency contact purposes; or

(C) that is necessary for the business to retain to administer benefits for another individual relating

to the individual under item (1) if used solely for the purposes of administering those benefits;

(14) personal data collected, processed, sold, or disclosed under the Illinois Insurance Code;

(15) data collected, processed, sold, or disclosed as part of a payment-only credit, check, or cash transaction where no data about consumers, as defined in Section 11, are retained;

(16) a State or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in the United States Code, Title 12, Section 1843(k);

(17) information that originates from, or is intermingled so as to be indistinguishable from, information described in clause (8) and that a person licensed under chapter 56 collects, processes, uses, or maintains in the same manner as is required under the laws and regulations specified in clause (8);

(18) an insurance company and an insurance producer that are regulated by the State under the Illinois Insurance Code, a third-party administrator of self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is principally engaged in financial activities, as described in the United States Code, Title 12, Section 1843(k), except that this clause does not apply to a person that, alone or in

combination with another person, establishes and maintains a self-insurance program that does not otherwise engage in the business of entering into policies of insurance;

(19) a small business, as defined by the United States Small Business Administration under the Code of Federal Regulations, Title 13, Part 121, except that a small business identified in this clause is subject to Section 17;

(20) a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance; and

(21) an air carrier subject to the federal Airline Deregulation Act, Public Law 95-504, only to the extent that an air carrier collects personal data related to prices, routes, or services and only to the extent that the provisions of the Airline Deregulation Act preempt the requirements of this Act.

Controllers that are in compliance with the Children's Online Privacy Protection Act, United States Code, Title 15, Sections 6501 to 6506, and implementing regulations, are deemed compliant with any obligation to obtain parental consent under this Act.

Section 13. Responsibility according to role.

(a) Controllers and processors are responsible for meeting the respective obligations established under this Act.

(b) Processors are responsible under this Act for adhering to the instructions of the controller and assisting the controller to meet the controller's obligations under this Act. Assistance under this subsection shall include the following:

(1) taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights under Section 14; and

(2) taking into account the nature of processing and the information available to the processor, the processor shall assist the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system under the Illinois Personal Information Protection Act and provide information to the controller necessary to enable the controller to conduct and document any data privacy and protection assessments required by Section 18.

(c) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the

type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also require that the processor:

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

(2) engage a subcontractor only (i) after providing the controller with an opportunity to object, and (ii) pursuant to a written contract in accordance with subsection (e) that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(d) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between the controller and the processor to implement the technical and organizational measures.

(e) Processing by a processor shall be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties.

The contract shall include the requirements imposed by this subsection, subsections (c) and (d), as well as the following requirements:

(1) at the choice of the controller, the processor shall 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;

(2) upon a reasonable request from the controller, the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this Act; and

(3) the processor shall allow for, and contribute to, reasonable assessments and inspections by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct, at least annually and at the processor's expense, an assessment of the processor's policies and technical and organizational measures in support of the obligations under this Act. The assessor must use an appropriate and accepted control standard or framework and assessment procedure for assessments as applicable, and shall provide a report of an assessment to the controller upon request.

(f) In no event shall any contract relieve a controller or a processor from the liabilities imposed on a controller or processor by virtue of the controller's or processor's roles

in the processing relationship under this Act.

(g) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in the person's processing of personal data pursuant to a controller's instructions, or that fails to adhere to a controller's instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing.

Section 14. Consumer personal data rights.

(a)(1) Consumer rights provided. Except as provided in this Act, a controller must comply with a request to exercise the consumer rights provided in this subdivision.

(2) A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access the categories of personal data the controller is processing.

(3) A consumer has the right to correct inaccurate personal data concerning the consumer taking into account the

nature of the personal data and the purposes of the processing of the personal data.

(4) A consumer has the right to delete personal data concerning the consumer.

(5) A consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

(6) A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of automated decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

(7) If a consumer's personal data is profiled in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the consumer has the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. The

consumer has the right to review the consumer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data taking into account the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

(8) A consumer has a right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead.

(b)(1) Exercising consumer rights. A consumer may exercise the rights set forth in this Section by submitting a request, at any time, to a controller specifying which rights the consumer wishes to exercise.

(2) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child may exercise the rights under this Act on the child's behalf.

(3) In the case of processing personal data concerning a consumer legally subject to guardianship under the Probate Act of 1975, the guardian of the consumer may exercise the rights under this Act on the consumer's behalf.

(4) A consumer may designate another person as the consumer's authorized agent to exercise the consumer's right

to opt out of the processing of the consumer's personal data for purposes of targeted advertising and sale under subsection (1), paragraph (f), on the consumer's behalf. A consumer may designate an authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension, or global device setting, indicating the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(c)(1) Universal opt-out mechanisms. A controller must allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer's personal data through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of the processing or sale. The platform, technology, or mechanism must:

(A) not unfairly disadvantage another controller;

(B) not make use of a default setting but require the consumer to make an affirmative, freely given, and unambiguous choice to opt out of the processing of the consumer's personal data;

(C) be consumer-friendly and easy to use by the

average consumer;

(D) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or State law or regulation; and

(E) enable the controller to accurately determine whether the consumer is an Illinois resident and whether the consumer has made a legitimate request to opt out of any sale of the consumer's personal data or targeted advertising. For purposes of this paragraph, the use of an Internet protocol address to estimate the consumer's location is sufficient to determine the consumer's residence.

(2) If a consumer's opt-out request is exercised through the platform, technology, or mechanism required under paragraph (a), and the request conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller must comply with the consumer's opt-out preference signal but may also notify the consumer of the conflict and provide the consumer a choice to confirm the controller-specific privacy setting or participation in the controller's program.

(3) The platform, technology, or mechanism required under paragraph (a) is subject to the requirements of subdivision 4.

(4) A controller that recognizes opt-out preference

signals that have been approved by other state laws or regulations is in compliance with this subdivision.

(d)(1) Controller response to consumer requests. Except as provided in this Act, a controller must comply with a request to exercise the rights pursuant to subdivision 1.

(2) A controller must provide one or more secure and reliable means for consumers to submit a request to exercise the consumer's rights under this Section. The means made available must take into account the ways in which consumers interact with the controller and the need for secure and reliable communication of the requests.

(3) A controller may not require a consumer to create a new account to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this Section.

(4) A controller must comply with a request to exercise the right in subsection (1), paragraph (f), as soon as feasibly possible, but no later than 45 days of receipt of the request.

(5) A controller must inform a consumer of any action taken on a request under subdivision 1 without undue delay and in any event within 45 days of receipt of the request. That period may be extended once by 45 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any extension within 45 days of receipt of the

request, together with the reasons for the delay.

(6) If a controller does not take action on a consumer's request, the controller must inform the consumer without undue delay and at the latest within 45 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in subdivision 5.

(7) Information provided under this Section must be provided by the controller free of charge up to twice annually to the consumer. If requests from a consumer are manifestly unfounded or excessive, in particular because of the repetitive character of the requests, the controller may either charge a reasonable fee to cover the administrative costs of complying with the request or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(8) A controller is not required to comply with a request to exercise any of the rights under subsection (1), paragraphs (b) to (e) and (h), if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request the provision of additional information reasonably necessary to authenticate the request. A controller is not required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an

opt-out request because the controller believes a request is fraudulent, the controller must notify the person who made the request that the request was denied because of the controller's belief that the request was fraudulent and state the controller's basis for that belief.

(9) In response to a consumer request under subdivision 1, a controller must not disclose the following information about a consumer but must instead inform the consumer with sufficient particularity that the controller has collected that type of information:

(A) Social Security number;

(B) driver's license number or other government-issued identification number;

(C) financial account number;

(D) health insurance account number or medical identification number;

(E) account password, security questions, or answers; or

(F) biometric data.

(10) In response to a consumer request under subdivision 1, a controller is not required to reveal any trade secret.

(11) A controller that has obtained personal data about a consumer from a source other than the consumer may comply with a consumer's request to delete the consumer's personal data pursuant to subsection (1), paragraph (d), by either:

(A) retaining a record of the deletion request,

retaining the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's 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 personal data for any purpose except for the purposes exempted pursuant to the provisions of this Act.

(e)(1) Appeal process required. A controller must establish an internal process in which a consumer may appeal a refusal to take action on a request to exercise any of the rights under subdivision 1 within a reasonable period of time after the consumer's receipt of the notice sent by the controller under subdivision 4, paragraph (f).

(2) The appeal process must be conspicuously available. The process must include the ease of use provisions in subdivision 3 applicable to submitting requests.

(3) Within 45 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal along with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days if reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any extension within 45 days of receipt of the appeal together with the reasons for the delay.

(4) When informing a consumer of any action taken or not

taken in response to an appeal pursuant to paragraph (c), the controller must provide a written explanation of the reasons for the controller's decision and clearly and prominently provide the consumer with information about how to file a complaint with the Attorney General. The controller must maintain records of all appeals and the controller's responses for at least 24 months and shall, upon written request by the Attorney General as part of an investigation, compile and provide a copy of the records to the Attorney General.

Section 15. Processing deidentified data or pseudonymous data.

(a) This Act does not require a controller or processor to do any of the following solely for purposes of complying with this Act:

(1) reidentify deidentified data;

(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; or

(3) comply with an authenticated consumer request to access, correct, delete, or port personal data under Section 14, subsection (1), if all of the following are true:

(A) 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;

(B) 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

(C) 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.

(b) The rights contained in Section 14, subsection (1), paragraphs (b) to (e) and (h), do not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(c) A controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject, and must take appropriate steps to address any breaches of contractual commitments.

(d) A processor or third party must not attempt to

identify the subjects of deidentified or pseudonymous data without the express authority of the controller that caused the data to be deidentified or pseudonymized.

(e) A controller, processor, or third party must not attempt to identify the subjects of data that has been collected with only pseudonymous identifiers.

Section 16. Responsibilities of controllers.

(a)(1) Transparency obligations. Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(A) the categories of personal data processed by the controller;

(B) the purposes for which the categories of personal data are processed;

(C) an explanation of the rights contained in Section 14 and how and where consumers may exercise those rights, including how a consumer may appeal a controller's action with regard to the consumer's request;

(D) the categories of personal data that the controller sells to or shares with third parties, if any;

(E) the categories of third parties, if any, with whom the controller sells or shares personal data;

(F) the controller's contact information, including an active email address or other online mechanism that the consumer may use to contact the controller;

(G) a description of the controller's retention policies for personal data; and

(H) the date the privacy notice was last updated.

(2) If a controller sells personal data to third parties, processes personal data for targeted advertising, or engages in profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the controller must disclose the processing in the privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale, processing, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer. This method may include but is not limited to an Internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.

(3) The privacy notice must be made available to the public in each language in which the controller provides a product or service that is subject to the privacy notice or carries out activities related to the product or service.

(4) The controller must provide the privacy notice in a manner that is reasonably accessible to and usable by individuals with disabilities.

(5) Whenever a controller makes a material change to the

controller's privacy notice or practices, the controller must notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide notification regarding material changes to affected consumers, taking into account available technology and the nature of the relationship.

(6) A controller is not required to provide a separate Illinois-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this Section.

(7) The privacy notice must be posted online through a conspicuous hyperlink using the word "privacy" on the controller's website home page or on a mobile application's app store page or download page. A controller that maintains an application on a mobile or other device shall also include a hyperlink to the privacy notice in the application's settings menu or in a similarly conspicuous and accessible location. A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including, but not limited to, mail.

(b)(1) Use of data. A controller must limit the collection

of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed, which must be disclosed to the consumer.

(2) Except as provided in this Act, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which the personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(3) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, including the maintenance of an inventory of the data that must be managed to exercise these responsibilities. The data security practices shall be appropriate to the volume and nature of the personal data at issue.

(4) Except as otherwise provided in this Act, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with the requirement of the Children's Online Privacy Protection Act, United States Code, Title 15, Sections 6501 to 6506, and its implementing regulations.

(5) A controller shall provide an effective mechanism for a consumer, or, in the case of the processing of personal data

concerning a known child, the child's parent or lawful guardian, to revoke previously given consent under this subsection. The mechanism provided shall be at least as easy as the mechanism by which the consent was previously given. Upon revocation of consent, a controller shall cease to process the applicable data as soon as practicable, but no later than 15 days after the receipt of the request.

(6) A controller may not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, without the consumer's consent, under circumstances in which the controller knows that the consumer is between the ages of 13 and 16.

(7) A controller may not retain personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under Section 19.

(c)(1) Nondiscrimination. A controller shall not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of: housing, employment, credit, or education; or the goods, services, facilities, privileges,

advantages, or accommodations of any place of public accommodation.

(2) A controller may not discriminate against a consumer for exercising any of the rights contained in this Act, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection does not: (i) require a controller to provide a good or service that requires the consumer's personal data that the controller does not collect or maintain; or (ii) 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 offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(d) Waiver of rights unenforceable. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this Act is contrary to public policy and is void and unenforceable.

Section 17. Requirements for small businesses.

(a) A small business, as defined by the United States Small Business Administration under the Code of Federal Regulations, Title 13, Part 121, that conducts business in Illinois or produces products or services that are targeted to

Illinois residents must not sell a consumer's sensitive data without the consumer's prior consent.

(b) Penalties and Attorney General enforcement procedures under Section 20 apply to a small business that violates this Section.

Section 18. Data privacy policies; data privacy and protection assessments.

(a) A controller must document and maintain a description of the policies and procedures the controller has adopted to comply with this Act. The description must include, where applicable:

(1) the name and contact information for the controller's chief privacy officer or other individual with primary responsibility for directing the policies and procedures implemented to comply with the provisions of this Act; and

(2) a description of the controller's data privacy policies and procedures that reflect the requirements in Section 16, and any policies and procedures designed to:

(i) reflect the requirements of this Act in the design of the controller's systems;

(ii) identify and provide personal data to a consumer as required by this Act;

(iii) establish, implement, and maintain reasonable administrative, technical, and physical

data security practices to protect the confidentiality, integrity, and accessibility of personal data, including the maintenance of an inventory of the data that must be managed to exercise the responsibilities under this item;

(iv) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed;

(v) prevent the retention of personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under Section 19; and

(vi) identify and remediate violations of this Act.

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

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

(2) the sale of personal data;

(3) the processing of sensitive data;

(4) any processing activities involving personal data that present a heightened risk of harm to consumers; and

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

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

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

(iii) 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

(iv) other substantial injury to consumers.

(c) A data privacy and protection assessment must take into account the type of personal data to be processed by the controller, including the extent to which the personal data are sensitive data, and the context in which the personal data are to be processed.

(d) A data privacy and protection assessment must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, 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 potential risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the

controller and the consumer whose personal data will be processed, must be factored into this assessment by the controller.

(e) A data privacy and protection assessment must include the description of policies and procedures required by subsection (a).

(f) As part of a civil investigative demand, the Attorney General may request, in writing, that a controller disclose any data privacy and protection assessment that is relevant to an investigation conducted by the Attorney General. The controller must make a data privacy and protection assessment available to the Attorney General upon a request made under this subsection. The Attorney General may evaluate the data privacy and protection assessments for compliance with this Act. Data privacy and protection assessments is nonpublic data that is data required by State or federal law that is: (1) not about an individual; (2) not accessible by the general public; and (3) accessible by the subject of the data. The disclosure. The disclosure of a data privacy and protection assessment under a request from the Attorney General under this subsection does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(g) Data privacy and protection assessments or risk assessments conducted by a controller for the purpose of compliance with other laws or regulations may qualify under

this Section if the assessments have a similar scope and effect.

(h) A single data protection assessment may address multiple sets of comparable processing operations that include similar activities.

Section 19. Limitations and applicability.

(a) The obligations imposed on controllers or processors under this Act do not restrict a controller's or a processor's ability to:

(1) comply with federal, State, or local laws, rules, or regulations, including, but not limited to, data retention requirements in State or federal law notwithstanding a consumer's request to delete personal data;

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

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

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

(5) provide a product or service specifically requested by a consumer; perform a contract to which the

consumer is a party, including fulfilling the terms of a written warranty; or take steps at the request of the consumer prior to entering into a contract;

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

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

(8) assist another controller, processor, or third party with any of the obligations under this subsection;

(9) engage in public or peer-reviewed scientific, historical, 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, human subjects research ethics review board, or a similar independent oversight entity that has determined:

(A) the research 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 any risks associated with reidentification; or

(10) process personal data for the benefit of the public in the areas of public health, community health, or population health, but only to the extent that the processing is:

(A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(B) under the responsibility of a professional individual who is subject to confidentiality obligations under federal, State, or local law.

(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) effectuate a product recall or identify and repair technical errors that impair existing or intended functionality;

(2) perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing 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; or

(3) conduct internal research to develop, improve, or repair products, services, or technology.

(c) The obligations imposed on controllers or processors under this Act do not apply if compliance by the controller or processor with this Act would violate an evidentiary privilege under Illinois law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Illinois law 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 recipient processes the personal data 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 not in violation of this Act for the obligations of the controller or processor from which the third-party controller or processor receives the personal data.

(e) Obligations imposed on controllers and processors

under this Act shall not:

(1) adversely affect the rights or freedoms of any persons, including exercising the right of free speech pursuant to the First Amendment of the United States Constitution; or

(2) apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

(f) Personal data that are processed by a controller pursuant to this Section may be processed solely to the extent that the processing is:

(1) necessary, reasonable, and proportionate to the purposes listed in this Section;

(2) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this Section; and

(3) insofar as possible, taking into account the nature and purpose of processing the personal data, subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers.

(g) If a controller processes personal data pursuant to 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 subsection (f).

(h) Processing personal data solely for the purposes expressly identified in subsection (a), clauses (1) to (7), does not, by itself, make an entity a controller with respect to the processing.

Section 20. Attorney General enforcement.

(a) If a controller or processor violates this Act, the Attorney General, before filing an enforcement action under subsection (b), must provide the controller or processor with a warning letter identifying the specific provisions of this Act the Attorney General alleges have been or are being violated. If, after 30 days of issuance of the warning letter, the Attorney General believes the controller or processor has failed to cure any alleged violation, the Attorney General may bring an enforcement action under subsection (b). This subsection expires January 1, 2028.

(b) The Attorney General may bring a civil action against a controller or processor to enforce a provision of this Act. If the State prevails in an action to enforce this Act, the State may, in addition to penalties provided by subsection (c) or other remedies provided by law, be allowed an amount determined by the court to be the reasonable value of all or part of the State's litigation expenses incurred.

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

(d) Nothing in this Act establishes a private right of action for a violation of this Act or any other law.

Section 95. Home rule. A unit of local government, including a home rule unit, may not regulate consumer data privacy. This Section is a denial and limitation of home rule powers and functions under subsection (g) of Section 6 of Article VII of the Illinois Constitution.

Section 97. Severability. If any provision of this Act or its application to any person or circumstance is held invalid, the invalidity of that provision or application does not affect other provisions or applications of this Act that can be given effect without the invalid provision or application.