HB5288

LRB10119835JLS69355b

101ST GENERAL ASSEMBLY

State of Illinois

2019 and 2020

HB5288

by Rep. Kelly M. Burke

SYNOPSIS AS INTRODUCED:

New Act
30 ILCS 105/5.930 new

Creates the Data Privacy Act. Provides for the regulation of the use and sale of data. Defines terms. Establishes consumer rights to copies of information held by persons who control and process data. Provides for the correction of inaccurate data. Provides for restrictions on the use of personal data. Provides for the enforcement of the Act by the Attorney General. Provides civil penalties. Preempts home rule and provides that the regulation of data use and privacy are exclusive powers and functions of the State. Creates the Consumer Privacy Fund as a special fund in the State treasury.

LRB101 19835 JLS 69355 b

A BILL FOR

AN ACT concerning regulation.

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

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

Section 5. Definitions. As used in this Act:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, another legal entity.

(2) "Business associate" has the same meaning as in Title 45 CFR, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996.

(3) "Business purpose" means the processing of personal data for the controller's or its processor's operational purposes, or other notified purposes, provided that the processing of personal data must be reasonably necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed or for another operational purpose that is compatible with the context in which the personal data was collected. Business purposes include:

(a) auditing related to a current interaction with the consumer and concurrent transactions including, but not

limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

(b) detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;

(c) identifying and repairing errors that impair existing or intended functionality;

(d) short-term, transient use, provided the personal data is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction including, but not limited to, the contextual customization of ads shown as part of the same interaction;

(e) maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;

(f) undertaking internal research for technological development; or

(g) authenticating a consumer's identity.

(4) "Child" means any natural person under 13 years of age.

(5) "Consent" means a clear affirmative act signifying a specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear

affirmative action.

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

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

(8) "Covered entity" has the meaning ascribed to that term in Title 45 CFR, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996.

(9)(a) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(b) Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker.

(c) The phrase "sells or licenses" does not include:

(i) a one-time or occasional sale of assets that is not part of the ordinary conduct of the business;

(ii) a sale or license of data that is merely incidental to the business; or

(iii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier.

(10) "Deidentified data" means:

(a) data that cannot be linked to a known natural person without additional information kept separately; or

(b) data (i) that has been modified to a degree that the risk of reidentification is small, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, and (iii) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls.

(11) "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

(12) "Health care facility" means a hospital, clinic, nursing home, laboratory, office, or similar place where a health care provider provides health care to patients.

(13) "Health care information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of

chemical base pairs. The term includes any required accounting of disclosures of health care information.

(14) "Health care provider" means a person who is licensed, certified, registered, or otherwise authorized by the law of this State to provide health care in the ordinary course of business or practice of a profession.

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

(16) "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. For these purposes, "publicly available information" means information that is lawfully made available from federal, State, or local government records.

(17) "Process" or "processing" means any collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(18) "Processor" means a natural or legal person that processes personal data on behalf of the controller.

(19) "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(20) "Protected health information" has the meaning ascribed to that term in Title 45 CFR, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996.

(21) "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

(22)(a) "Sale", "sell", or "sold" means the exchange of personal data for monetary consideration by the controller to a third party for purposes of licensing or selling personal data at the third party's discretion to additional third parties.

(b) "Sale" does not include the following: (i) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(23) "Sensitive data" means: (a) personal data revealing

racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; or (c) the personal data of a known child.

(24) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's activities across nonaffiliated websites, applications, or online services to predict user preferences or interests. It does not include advertising to a consumer based upon the consumer's visits to a website, application, or online service that a reasonable consumer would believe to be associated with the publisher where the ad is placed based on common branding, trademarks, or other indicia of common ownership, or in response to the consumer's request for information or feedback.

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

(26) "Verified request" means the process through which a consumer may submit a request to exercise a right or rights set forth in this Act, and by which a controller can reasonably authenticate the request and the consumer making the request using commercially reasonable means.

Section 10. Jurisdictional scope.

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

(a) Controls or processes personal data of 100,000 consumers or more.

(b) Derives over 50% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.

(2) This Act does not apply to:

(a) State and local governments.

(b) Municipal corporations.

(c) Information that meets the definition of:

(i) protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996 and related regulations;

(ii) patient identifying information for purposes of 42 CFR Part 2, established pursuant to 42 U.S.C. 290 dd-2;

(iii) identifiable private information for purposes of the federal policy for the protection of human subjects, 45 CFR Part 46, or identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the

International Council for Harmonisation, or the protection of human subjects under 21 CFR Parts 50 and 56;

(iv) information and documents created specifically for, and collected and maintained by:

(A) a quality improvement committee of a health care facility;

(B) a peer review committee for purposes disciplinary actions involving a member of a licensed profession;

(C) a quality assurance committee for purposes of assisted living facilities and nursing homes; or

(D) a health care facility, for reporting of health care-associated infections or a notification of an adverse health incidents;

(v) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, and related regulations; or

(vi) patient safety work product information for purposes of 42 CFR Part 3, established pursuant to 42 U.S.C. 299b-21-26.

(d) Information maintained in the same manner as information under paragraph (c) of subsection (2) by:

(i) a covered entity or business associate as defined by the Health Insurance Portability and

Accountability Act of 1996 and related regulations;

(ii) a health care facility or health care provider; or

(iii) a program or a qualified service organization as defined in 42 CFR Part 2, established pursuant to 42 U.S.C. 290dd-2.

(e) Personal data provided to, from, or held by a consumer reporting agency as defined in 15 U.S.C. 1681a(f), and use of that data is in compliance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(f) Personal data collected, processed, sold, or disclosed pursuant to 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.

(g) Personal data collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.), if the collection, processing, sale, or disclosure is in compliance with that law.

(h) Data maintained for employment records purposes.

Section 15. Responsibility according to role.

(1) Controllers are responsible for meeting the obligations established under this Act.

(2) Processors are responsible under this Act for adhering

to the instructions of the controller and assisting the controller to meet its obligations under this Act.

(3) Processing by a processor is governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

Section 20. Consumer rights. Controllers shall facilitate verified requests to exercise the consumer rights set forth in subsections (1) through (6) of this Section.

(1) Upon a verified request from a consumer, a controller must confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data that the controller maintains in identifiable form concerning the consumer.

(a) Upon a verified request from a consumer, a controller must provide a copy of the personal data that the controller maintains in identifiable form undergoing processing. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information must be provided

in a commonly used electronic form.

(b) This subsection does not adversely affect the rights or freedoms of others.

(2) Upon a verified request from a consumer, the controller, without undue delay, must correct inaccurate personal data that the controller maintains in identifiable form concerning the consumer. Taking into account the business purposes of the processing, the controller must complete incomplete personal data, including by means of providing a supplementary statement where appropriate.

(3)(a) Upon a verified request from a consumer, a controller must delete, without undue delay, the consumer's personal data that the controller maintains in identifiable form if one of the following grounds applies:

(i) The personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer.

(ii) For processing that requires consent under subsection (3) of Section 30, the consumer withdraws consent to processing and there are no business purposes for the processing.

(iii) The consumer objects to the processing pursuant to subsection (6) of this Section and: (A) there are no business purposes for processing the personal data for the controller, the consumer whose personal data is being processed, or the public, for which the processing is

necessary; or (B) the processing is for targeted advertising.

(iv) The personal data has been unlawfully processed.

(v) The personal data must be deleted to comply with a legal obligation under federal, State, or local law to which the controller is subject.

(b) Where the controller is obliged to delete personal data that the controller maintains in identifiable form under this Section and that has been disclosed to third parties by the controller, including data brokers that received the personal data through a sale, the controller must take reasonable steps, which may include technical measures, to inform other controllers of which it is aware that are processing such personal data, and that received such personal data from the controller or are processing such personal data on behalf of the controller, that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation must take into account available technology and cost of implementation.

(c) This subsection does not apply to the extent processing is necessary:

(i) for exercising the right of free speech;

(ii) for compliance with a legal obligation that requires processing of personal data by federal, State, or local law, or regulation to which the controller is subject

or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) for reasons of public interest in the area of public health, where the processing: (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is under the responsibility of a professional subject to confidentiality obligations under federal, State, or local law;

(iv) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing;

(v) for the establishment, exercise, or defense of legal claims;

(vi) to detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity; or

(vii) for a data broker that received the personal data from third parties and is acting as a controller, solely to prevent the personal data from reappearing in the future, in which case the controller shall instead comply with the requirements in subsection (4) of this Section.

(4)(a) Upon a verified request from a consumer, the

controller must restrict processing of personal data that the controller maintains in identifiable form if the purpose for which the personal data is: (i) not consistent with a purpose for which the personal data was collected; (ii) not consistent with a purpose disclosed to the consumer at the time of collection or authorization; or (iii) unlawful.

(b) Where personal data is subject to a restriction of processing under this subsection, the personal data must, with the exception of storage, only be processed: (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; (iii) for the protection of the rights of another natural or legal person; (iv) for reasons of important public interest under federal, State, or local law; (v) to provide products or services requested by the consumer; or (vi) for another purpose set forth in paragraph (c) of subsection (3).

(c) A consumer who has obtained restriction of processing pursuant to this subsection must be informed by the controller before the restriction of processing is lifted.

(5)(a) Upon a verified request from a consumer, the controller must provide to the consumer, if technically feasible and commercially reasonable, any personal data that the controller maintains in identifiable form concerning the consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if:

(i)(A) the processing of such personal data requires

consent under subsection (3) of Section 30, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and

(ii) the processing is carried out by automated means.

(b) Requests for personal data under this subsection must be without prejudice to the other rights granted under this Act.

(c) The rights provided in this subsection do not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and must not adversely affect the rights of others.

(6)(a) A consumer may object through a verified request, on grounds relating to the consumer's particular situation, at any time to processing of personal data concerning such consumer.

(b) When a consumer objects to the processing of their personal data for targeted advertising, which includes the sale of personal data concerning the consumer to third parties for purposes of targeted advertising, the controller must no longer process the personal data subject to the objection for such purpose and must take reasonable steps to communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for such purposes to any third

parties to whom the controller sold the consumer's personal data for such purposes. Third parties must honor objection requests pursuant to this subsection received from third-party controllers.

(c) If a consumer objects to processing for any purposes, other than targeted advertising, the controller may continue processing the personal data subject to the objection if the controller can demonstrate a legitimate ground to process such personal data that overrides the potential risks to the rights of the consumer associated with the processing, or if another exemption in this Act applies.

(7) A controller must communicate any correction, deletion, or restriction of processing carried out in accordance with subsections (2), (3), or (4) of this Section to each third-party recipient to whom the controller knows the personal data has been disclosed, including third parties that received the data through a sale, within one year preceding the verified request unless this proves functionally impractical, technically infeasible, or involves disproportionate effort, or the controller knows or is informed by the third party that the third party is not continuing to use the personal data. The controller must inform the consumer about third-party recipients or categories with whom the controller shares personal information, if any, if the consumer requests such information.

(8) A controller must provide information on action taken

on a verified request under subsections (1) through (6) of this Section without undue delay and in any event within 30 days of receipt of the request. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within 30 days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information must be provided by electronic means where possible, unless otherwise requested by the consumer.

(a) If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within 30 days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) Information provided under this Section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating

the manifestly unfounded or excessive character of the request.

(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request under subsections (1) through (6) of this Section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

Section 25. Transparency.

(1) Controllers must be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that includes:

(a) the categories of personal data collected by the controller;

(b) the purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) the rights that consumers may exercise pursuant to Section 20, if any;

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

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

(2) If a controller sells personal data to data brokers or processes personal data for targeted advertising, it must

disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and conspicuous manner.

Section 30. Risk assessments.

(1) Controllers must conduct, to the extent not previously conducted, a risk assessment of each of their processing activities involving personal data and an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. Such risk assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data is sensitive data or otherwise sensitive in nature, and the context in which the personal data is to be processed.

(2) Risk assessments conducted under subsection (1) 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 such processing, as mitigated by safeguards that can be employed by the controller to reduce such 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 factor into this assessment by the controller.

(3) If the risk assessment conducted under subsection (1) determines that the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer or if another exemption under this Act applies. To the extent the controller seeks consumer consent for processing, such consent shall be as easy to withdraw as to give.

(4) Processing for a business purpose shall be presumed to be permissible unless: (a) it involves the processing of sensitive data; and (b) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.

(5) The controller must make the risk assessment available to the Attorney General upon request. Risk assessments are confidential and exempt from public inspection and copying under the Freedom of Information Act.

Section 35. Deidentified data. A controller or processor that uses deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject, and must take appropriate steps to address any breaches of contractual commitments.

Section 40. Exemptions.

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

(a) comply with federal, State, or local laws, rules, or regulations;

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

(c) 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 law;

(d) investigate, exercise, or defend legal claims;

(e) prevent or detect identity theft, fraud, or other criminal activity or verify identities;

(f) perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

(g) protect the vital interests of the consumer or of another natural person;

(h) perform a task carried out in the public interest or in the exercise of official authority vested in the controller;

(i) process personal data of a consumer for one or more specific purposes where the consumer has given their consent to the processing; or

(j) prevent, detect, 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.

(2) The obligations imposed on controllers or processors under this Act do not apply where 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.

(3) 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, including under Section 45, if the recipient processes such 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 is likewise not liable under this Act, including under Section 45, for the obligations of a controller or processor to which it provides services.

(4) This Act does not require a controller or processor to do the following:

(a) Reidentify deidentified data.

(b) Retain, link, or combine personal data concerning a consumer that it would not otherwise retain, link, or combine in the ordinary course of business.

(c) Comply with a request to exercise any of the rights under subsections (1) through (6) of Section 20 if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

(5) Obligations imposed on controllers and processors under this Act do not:

(a) adversely affect the rights or freedoms of any persons; or

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

Section 45. Liability.

(1) This Act does not serve as the basis for a private right of action under this Act or any other law.

(2) Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this Act, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

Section 50. Enforcement.

(1) The General Assembly finds that the practices covered by this Act are matters vitally affecting the public interest for the purpose of applying the Consumer Fraud and Deceptive Business Practices Act. A violation of this Act is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the Consumer Fraud and Deceptive Business Practices Act.

(2) The Attorney General may bring an action in the name of the State, or as parens patriae on behalf of persons residing in the State, to enforce this Act.

(3) A controller or processor is in violation of this Act if it fails to cure any alleged violation of Sections 20 through 40 within 30 days after receiving notice of alleged noncompliance. Any controller or processor that violates this Act is subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

(4) The Consumer Privacy Fund is created as a special fund in the State treasury. All receipts from the imposition of civil penalties under this Act must be deposited into the Fund. Moneys in the Fund may be spent only after appropriation. Expenditures from the Fund may be used only to fund privacy and data protection activities performed by the State Chief

Information Officer.

Section 55. Home rule. The regulation of data use and privacy is an exclusive power and function of the State. A unit of local government, including home rule unit, may not regulate data use and privacy. This Section is a denial and limitation of home rule powers and functions under subsection (h) of Section 6 of Article VII of the Illinois Constitution.

Section 90. The State Finance Act is amended by adding Section 5.930 as follows:

(30 ILCS 105/5.930 new)

Sec. 5.930. The Consumer Privacy Fund.