SB2263

101ST GENERAL ASSEMBLY

State of Illinois

2019 and 2020

SB2263

Introduced 5/31/2019, by Sen. Don Harmon

SYNOPSIS AS INTRODUCED:

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. Effective immediately.

FISCAL NOTE ACT
MAY APPLY

HOME RULE NOTE
ACT MAY APPLY

A BILL FOR

1   AN ACT concerning regulation.

2   **Be it enacted by the People of the State of Illinois,**

3   **represented in the General Assembly:**

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

5   Privacy Act.

6   Section 5. Definitions. As used in this Act:

7   (1) "Affiliate" means a legal entity that controls, is

8   controlled by, or is under common control with, another legal

9   entity.

10   (2) "Business associate" has the same meaning as in Title

11   45 CFR, established pursuant to the federal Health Insurance

12   Portability and Accountability Act of 1996.

13   (3) "Business purpose" means the processing of personal

14   data for the controller's or its processor's operational

15   purposes, or other notified purposes, provided that the

16   processing of personal data must be reasonably necessary and

17   proportionate to achieve the operational purposes for which the

18   personal data was collected or processed or for another

19   operational purpose that is compatible with the context in

20   which the personal data was collected. Business purposes

21   include:

22   (a) auditing related to a current interaction with the

23   consumer and concurrent transactions including, but not

1   limited to, counting ad impressions, verifying positioning

2   and quality of ad impressions, and auditing compliance with

3   this specification and other standards;

4   (b) detecting security incidents, protecting against

5   malicious, deceptive, fraudulent, or illegal activity, and

6   prosecuting those responsible for that activity;

7   (c) identifying and repairing errors that impair

8   existing or intended functionality;

9   (d) short-term, transient use, provided the personal

10   data is not disclosed to another third party and is not

11   used to build a profile about a consumer or otherwise alter

12   an individual consumer's experience outside the current

13   interaction including, but not limited to, the contextual

14   customization of ads shown as part of the same interaction;

15   (e) maintaining or servicing accounts, providing

16   customer service, processing or fulfilling orders and

17   transactions, verifying customer information, processing

18   payments, or providing financing;

19   (f) undertaking internal research for technological

20   development; or

21   (g) authenticating a consumer's identity.

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

23   (5) "Consent" means a clear affirmative act signifying a

24   specific, informed, and unambiguous indication of a consumer's

25   agreement to the processing of personal data relating to the

26   consumer, such as by a written statement or other clear

1   affirmative action.

2   (6) "Consumer" means a natural person who is an Illinois

3   resident acting only in an individual or household context. It

4   does not include a natural person acting in a commercial or

5   employment context.

6   (7) "Controller" means the natural or legal person which,

7   alone or jointly with others, determines the purposes and means

8   of the processing of personal data.

9   (8) "Covered entity" has the meaning ascribed to that term

10   in Title 45 CFR, established pursuant to the federal Health

11   Insurance Portability and Accountability Act of 1996.

12   (9)(a) "Data broker" means a business, or unit or units of

13   a business, separately or together, that knowingly collects and

14   sells or licenses to third parties the brokered personal

15   information of a consumer with whom the business does not have

16   a direct relationship.

17   (b) Providing publicly available information through

18   real-time or near real-time alert services for health or safety

19   purposes, and the collection and sale or licensing of brokered

20   personal information incidental to conducting those

21   activities, does not qualify the business as a data broker.

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

23   (i) a one-time or occasional sale of assets that is not

24   part of the ordinary conduct of the business;

25   (ii) a sale or license of data that is merely

26   incidental to the business; or

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

5   (10) "Deidentified data" means:

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

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

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

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

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

1   chemical base pairs. The term includes any required accounting

2   of disclosures of health care information.

3   (14) "Health care provider" means a person who is licensed,

4   certified, registered, or otherwise authorized by the law of

5   this State to provide health care in the ordinary course of

6   business or practice of a profession.

7   (15) "Identified or identifiable natural person" means a

8   person who can be readily identified, directly or indirectly.

9   (16) "Personal data" means any information that is linked

10 or reasonably linkable to an identified or identifiable natural

11 person. Personal data does not include deidentified data or

12 publicly available information. For these purposes, "publicly

13 available information" means information that is lawfully made

14 available from federal, State, or local government records.

15   (17) "Process" or "processing" means any collection, use,

16 storage, disclosure, analysis, deletion, or modification of

17 personal data.

18   (18) "Processor" means a natural or legal person that

19 processes personal data on behalf of the controller.

20   (19) "Profiling" means any form of automated processing of

21 personal data consisting of the use of personal data to

22 evaluate certain personal aspects relating to a natural person,

23 in particular to analyze or predict aspects concerning that

24 natural person's economic situation, health, personal

25 preferences, interests, reliability, behavior, location, or

26 movements.

1   (20) "Protected health information" has the meaning

2   ascribed to that term in Title 45 CFR, established pursuant to

3   the federal Health Insurance Portability and Accountability

4   Act of 1996.

5   (21) "Restriction of processing" means the marking of

6   stored personal data with the aim of limiting the processing of

7   such personal data in the future.

8   (22)(a) "Sale", "sell", or "sold" means the exchange of

9   personal data for monetary consideration by the controller to a

10   third party for purposes of licensing or selling personal data

11   at the third party's discretion to additional third parties.

12   (b) "Sale" does not include the following: (i) the

13   disclosure of personal data to a processor who processes the

14   personal data on behalf of the controller; (ii) the disclosure

15   of personal data to a third party with whom the consumer has a

16   direct relationship for purposes of providing a product or

17   service requested by the consumer or otherwise in a manner that

18   is consistent with a consumer's reasonable expectations

19   considering the context in which the consumer provided the

20   personal data to the controller; (iii) the disclosure or

21   transfer of personal data to an affiliate of the controller; or

22   (iv) the disclosure or transfer of personal data to a third

23   party as an asset that is part of a merger, acquisition,

24   bankruptcy, or other transaction in which the third party

25   assumes control of all or part of the controller's assets.

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

1 racial or ethnic origin, religious beliefs, mental or physical

2 health condition or diagnosis, or sex life or sexual

3 orientation; (b) the processing of genetic or biometric data

4 for the purpose of uniquely identifying a natural person; or

5 (c) the personal data of a known child.

6   (24) "Targeted advertising" means displaying

7 advertisements to a consumer where the advertisement is

8 selected based on personal data obtained or inferred over time

9 from a consumer's activities across nonaffiliated websites,

10 applications, or online services to predict user preferences or

11 interests. It does not include advertising to a consumer based

12 upon the consumer's visits to a website, application, or online

13 service that a reasonable consumer would believe to be

14 associated with the publisher where the ad is placed based on

15 common branding, trademarks, or other indicia of common

16 ownership, or in response to the consumer's request for

17 information or feedback.

18   (25) "Third party" means a natural or legal person, public

19 authority, agency, or body other than the consumer, controller,

20 or an affiliate of the processor of the controller.

21   (26) "Verified request" means the process through which a

22 consumer may submit a request to exercise a right or rights set

23 forth in this Act, and by which a controller can reasonably

24 authenticate the request and the consumer making the request

25 using commercially reasonable means.

1   Section 10. Jurisdictional scope.

2   (1) This Act applies to legal entities that conduct

3   business in Illinois or produce products or services that are

4   intentionally targeted to residents of Illinois, and that

5   satisfy one or more of the following thresholds:

6   (a) Controls or processes personal data of 100,000

7   consumers or more.

8   (b) Derives over 50% of gross revenue from the sale of

9   personal data and processes or controls personal data of

10   25,000 consumers or more.

11   (2) This Act does not apply to:

12   (a) State and local governments.

13   (b) Municipal corporations.

14   (c) Information that meets the definition of:

15   (i) protected health information for purposes of

16   the federal Health Insurance Portability and

17   Accountability Act of 1996 and related regulations;

18   (ii) patient identifying information for purposes

19   of 42 CFR Part 2, established pursuant to 42 U.S.C. 290

20   dd-2;

21   (iii) identifiable private information for

22   purposes of the federal policy for the protection of

23   human subjects, 45 CFR Part 46, or identifiable private

24   information that is otherwise information collected as

25   part of human subjects research pursuant to the good

26   clinical practice guidelines issued by the

1   International Council for Harmonisation, or the

2   protection of human subjects under 21 CFR Parts 50 and

3   56;

4   (iv) information and documents created

5   specifically for, and collected and maintained by:

6   (A) a quality improvement committee of a

7   health care facility;

8   (B) a peer review committee for purposes

9   disciplinary actions involving a member of a

10   licensed profession;

11   (C) a quality assurance committee for purposes

12   of assisted living facilities and nursing homes;

13   or

14   (D) a health care facility, for reporting of

15   health care-associated infections or a

16   notification of an adverse health incidents;

17   (v) information and documents created for purposes

18   of the federal Health Care Quality Improvement Act of

19   1986, and related regulations; or

20   (vi) patient safety work product information for

21   purposes of 42 CFR Part 3, established pursuant to 42

22   U.S.C. 299b-21-26.

23   (d) Information maintained in the same manner as

24 information under paragraph (c) of subsection (2) by:

25   (i) a covered entity or business associate as

26   defined by the Health Insurance Portability and

1   Accountability Act of 1996 and related regulations;

2   (ii) a health care facility or health care

3   provider; or

4   (iii) a program or a qualified service

5   organization as defined in 42 CFR Part 2, established

6   pursuant to 42 U.S.C. 290dd-2.

7   (e) Personal data provided to, from, or held by a

8 consumer reporting agency as defined in 15 U.S.C. 1681a(f),

9 and use of that data is in compliance with the federal Fair

10 Credit Reporting Act (15 U.S.C. 1681 et seq.).

11   (f) Personal data collected, processed, sold, or

12 disclosed pursuant to the federal Gramm-Leach-Bliley Act

13 (Public Law 106-102), and implementing regulations, if the

14 collection, processing, sale, or disclosure is in

15 compliance with that law.

16   (g) Personal data collected, processed, sold, or

17 disclosed pursuant to the federal Driver's Privacy

18 Protection Act of 1994 (18 U.S.C. 2721 et seq.), if the

19 collection, processing, sale, or disclosure is in

20 compliance with that law.

21   (h) Data maintained for employment records purposes.

22   Section 15. Responsibility according to role.

23   (1) Controllers are responsible for meeting the

24 obligations established under this Act.

25   (2) Processors are responsible under this Act for adhering

1   to   the   instructions   of   the   controller   and   assisting   the

2   controller to meet its obligations under this Act.

3   (3) Processing by a processor is governed by a contract

4   between the controller and the processor that is binding on the

5   processor and that sets out the processing instructions to

6   which the processor is bound.

7   Section 20. Consumer rights. Controllers shall facilitate

8   verified requests to exercise the consumer rights set forth in

9   subsections (1) through (6) of this Section.

10   (1) Upon a verified request from a consumer, a controller

11 must confirm whether or not personal data concerning the

12 consumer is being processed by the controller, including

13 whether such personal data is sold to data brokers, and, where

14 personal data concerning the consumer is being processed by the

15 controller, provide access to such personal data that the

16 controller maintains in identifiable form concerning the

17 consumer.

18   (a) Upon a verified request from a consumer, a

19   controller must provide a copy of the personal data that

20   the controller maintains in identifiable form undergoing

21   processing. For any further copies requested by the

22   consumer, the controller may charge a reasonable fee based

23   on administrative costs. Where the consumer makes the

24   request by electronic means, and unless otherwise

25   requested by the consumer, the information must be provided

1   in a commonly used electronic form.

2   (b) This subsection does not adversely affect the

3   rights or freedoms of others.

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

5   controller, without undue delay, must correct inaccurate

6   personal data that the controller maintains in identifiable

7   form concerning the consumer. Taking into account the business

8   purposes of the processing, the controller must complete

9   incomplete personal data, including by means of providing a

10   supplementary statement where appropriate.

11   (3)(a) Upon a verified request from a consumer, a

12   controller must delete, without undue delay, the consumer's

13   personal data that the controller maintains in identifiable

14   form if one of the following grounds applies:

15   (i) The personal data is no longer necessary for a

16   business purpose, including the provision of a product or

17   service to the consumer.

18   (ii) For processing that requires consent under

19   subsection (3) of Section 30, the consumer withdraws

20   consent to processing and there are no business purposes

21   for the processing.

22   (iii) The consumer objects to the processing pursuant

23   to subsection (6) of this Section and: (A) there are no

24   business purposes for processing the personal data for the

25   controller, the consumer whose personal data is being

26   processed, or the public, for which the processing is

1   necessary; or (B) the processing is for targeted

2   advertising.

3   (iv) The personal data has been unlawfully processed.

4   (v) The personal data must be deleted to comply with a

5   legal obligation under federal, State, or local law to

6   which the controller is subject.

7   (b) Where the controller is obliged to delete personal data

8   that the controller maintains in identifiable form under this

9   Section and that has been disclosed to third parties by the

10   controller, including data brokers that received the personal

11   data through a sale, the controller must take reasonable steps,

12   which may include technical measures, to inform other

13   controllers of which it is aware that are processing such

14   personal data, and that received such personal data from the

15   controller or are processing such personal data on behalf of

16   the controller, that the consumer has requested the deletion by

17   the other controllers of any links to, or copy or replication

18   of, the personal data. Compliance with this obligation must

19   take into account available technology and cost of

20   implementation.

21   (c) This subsection does not apply to the extent processing

22   is necessary:

23   (i) for exercising the right of free speech;

24   (ii) for compliance with a legal obligation that

25   requires processing of personal data by federal, State, or

26   local law, or regulation to which the controller is subject

1   or for the performance of a task carried out in the public

2   interest or in the exercise of official authority vested in

3   the controller;

4   (iii) for reasons of public interest in the area of

5   public health, where the processing: (A) is subject to

6   suitable and specific measures to safeguard the rights of

7   the consumer; and (B) is under the responsibility of a

8   professional subject to confidentiality obligations under

9   federal, State, or local law;

10   (iv) for archiving purposes in the public interest,

11   scientific or historical research purposes, or statistical

12   purposes, where the deletion of such personal data is

13   likely to render impossible or seriously impair the

14   achievement of the objectives of the processing;

15   (v) for the establishment, exercise, or defense of

16   legal claims;

17   (vi) to detect or respond to security incidents,

18   protect against malicious, deceptive, fraudulent, or

19   illegal activity, or identify, investigate, or prosecute

20   those responsible for that activity; or

21   (vii) for a data broker that received the personal data

22   from third parties and is acting as a controller, solely to

23   prevent the personal data from reappearing in the future,

24   in which case the controller shall instead comply with the

25   requirements in subsection (4) of this Section.

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

1   controller must restrict processing of personal data that the

2   controller maintains in identifiable form if the purpose for

3   which the personal data is: (i) not consistent with a purpose

4   for which the personal data was collected; (ii) not consistent

5   with a purpose disclosed to the consumer at the time of

6   collection or authorization; or (iii) unlawful.

7   (b) Where personal data is subject to a restriction of

8   processing under this subsection, the personal data must, with

9   the exception of storage, only be processed: (i) with the

10   consumer's consent; (ii) for the establishment, exercise, or

11   defense of legal claims; (iii) for the protection of the rights

12   of another natural or legal person; (iv) for reasons of

13   important public interest under federal, State, or local law;

14   (v) to provide products or services requested by the consumer;

15   or (vi) for another purpose set forth in paragraph (c) of

16   subsection (3).

17   (c) A consumer who has obtained restriction of processing

18   pursuant to this subsection must be informed by the controller

19   before the restriction of processing is lifted.

20   (5)(a) Upon a verified request from a consumer, the

21   controller must provide to the consumer, if technically

22   feasible and commercially reasonable, any personal data that

23   the controller maintains in identifiable form concerning the

24   consumer that such consumer has provided to the controller in a

25   structured, commonly used, and machine-readable format if:

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

1   consent under subsection (3) of Section 30, (B) the

2   processing of such personal data is necessary for the

3   performance of a contract to which the consumer is a party,

4   or (C) in order to take steps at the request of the

5   consumer prior to entering into a contract; and

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

7   (b) Requests for personal data under this subsection must

8   be without prejudice to the other rights granted under this

9   Act.

10   (c) The rights provided in this subsection do not apply to

11   processing necessary for the performance of a task carried out

12   in the public interest or in the exercise of official authority

13   vested in the controller, and must not adversely affect the

14   rights of others.

15   (6)(a) A consumer may object through a verified request, on

16   grounds relating to the consumer's particular situation, at any

17   time to processing of personal data concerning such consumer.

18   (b) When a consumer objects to the processing of their

19   personal data for targeted advertising, which includes the sale

20   of personal data concerning the consumer to third parties for

21   purposes of targeted advertising, the controller must no longer

22   process the personal data subject to the objection for such

23   purpose and must take reasonable steps to communicate the

24   consumer's objection, unless it proves impossible or involves

25   disproportionate effort, regarding any further processing of

26   the consumer's personal data for such purposes to any third

1   parties to whom the controller sold the consumer's personal

2   data for such purposes. Third parties must honor objection

3   requests pursuant to this subsection received from third-party

4   controllers.

5   (c) If a consumer objects to processing for any purposes,

6   other than targeted advertising, the controller may continue

7   processing the personal data subject to the objection if the

8   controller can demonstrate a legitimate ground to process such

9   personal data that overrides the potential risks to the rights

10 of the consumer associated with the processing, or if another

11 exemption in this Act applies.

12   (7) A controller must communicate any correction,

13 deletion, or restriction of processing carried out in

14 accordance with subsections (2), (3), or (4) of this Section to

15 each third-party recipient to whom the controller knows the

16 personal data has been disclosed, including third parties that

17 received the data through a sale, within one year preceding the

18 verified request unless this proves functionally impractical,

19 technically infeasible, or involves disproportionate effort,

20 or the controller knows or is informed by the third party that

21 the third party is not continuing to use the personal data. The

22 controller must inform the consumer about third-party

23 recipients or categories with whom the controller shares

24 personal information, if any, if the consumer requests such

25 information.

26   (8) A controller must provide information on action taken

1   on a verified request under subsections (1) through (6) of this

2   Section without undue delay and in any event within 30 days of

3   receipt of the request. That period may be extended by 60

4   additional days where reasonably necessary, taking into

5   account the complexity and number of the requests. The

6   controller must inform the consumer of any such extension

7   within 30 days of receipt of the request, together with the

8   reasons for the delay. Where the consumer makes the request by

9   electronic means, the information must be provided by

10 electronic means where possible, unless otherwise requested by

11 the consumer.

12   (a) If a controller does not take action on the request

13   of a consumer, the controller must inform the consumer

14   without undue delay and at the latest within 30 days of

15   receipt of the request of the reasons for not taking action

16   and any possibility for internal review of the decision by

17   the controller.

18   (b) Information provided under this Section must be

19   provided by the controller free of charge to the consumer.

20   Where requests from a consumer are manifestly unfounded or

21   excessive, in particular because of their repetitive

22   character, the controller may either: (i) charge a

23   reasonable fee taking into account the administrative

24   costs of providing the information or communication or

25   taking the action requested; or (ii) refuse to act on the

26   request. The controller bears the burden of demonstrating

1   the manifestly unfounded or excessive character of the

2   request.

3   (c) Where the controller has reasonable doubts

4   concerning the identity of the consumer making a request

5   under subsections (1) through (6) of this Section, the

6   controller may request the provision of additional

7   information necessary to confirm the identity of the

8   consumer.

9   Section 25. Transparency.

10   (1) Controllers must be transparent and accountable for

11   their processing of personal data, by making available in a

12   form that is reasonably accessible to consumers a clear,

13   meaningful privacy notice that includes:

14   (a) the categories of personal data collected by the

15   controller;

16   (b) the purposes for which the categories of personal

17   data is used and disclosed to third parties, if any;

18   (c) the rights that consumers may exercise pursuant to

19   Section 20, if any;

20   (d) the categories of personal data that the controller

21   shares with third parties, if any; and

22   (e) the categories of third parties, if any, with whom

23   the controller shares personal data.

24   (2) If a controller sells personal data to data brokers or

25   processes personal data for targeted advertising, it must

1   disclose such processing, as well as the manner in which a

2   consumer may exercise the right to object to such processing,

3   in a clear and conspicuous manner.

4   Section 30. Risk assessments.

5   (1) Controllers must conduct, to the extent not previously

6   conducted, a risk assessment of each of their processing

7   activities involving personal data and an additional risk

8   assessment any time there is a change in processing that

9   materially increases the risk to consumers. Such risk

10   assessments must take into account the type of personal data to

11   be processed by the controller, including the extent to which

12   the personal data is sensitive data or otherwise sensitive in

13   nature, and the context in which the personal data is to be

14   processed.

15   (2) Risk assessments conducted under subsection (1) must

16   identify and weigh the benefits that may flow directly and

17   indirectly from the processing to the controller, consumer,

18   other stakeholders, and the public, against the potential risks

19   to the rights of the consumer associated with such processing,

20   as mitigated by safeguards that can be employed by the

21   controller to reduce such risks. The use of deidentified data

22   and the reasonable expectations of consumers, as well as the

23   context of the processing and the relationship between the

24   controller and the consumer whose personal data will be

25   processed, must factor into this assessment by the controller.

1   (3) If the risk assessment conducted under subsection (1)

2   determines that the potential risks of privacy harm to

3   consumers are substantial and outweigh the interests of the

4   controller, consumer, other stakeholders, and the public in

5   processing the personal data of the consumer, the controller

6   may only engage in such processing with the consent of the

7   consumer or if another exemption under this Act applies. To the

8   extent the controller seeks consumer consent for processing,

9   such consent shall be as easy to withdraw as to give.

10   (4) Processing for a business purpose shall be presumed to

11   be permissible unless: (a) it involves the processing of

12   sensitive data; and (b) the risk of processing cannot be

13   reduced through the use of appropriate administrative and

14   technical safeguards.

15   (5) The controller must make the risk assessment available

16   to the Attorney General upon request. Risk assessments are

17   confidential and exempt from public inspection and copying

18   under the Freedom of Information Act.

19   Section 35. Deidentified data. A controller or processor

20   that uses deidentified data must exercise reasonable oversight

21   to monitor compliance with any contractual commitments to which

22   the deidentified data is subject, and must take appropriate

23   steps to address any breaches of contractual commitments.

24   Section 40. Exemptions.

1   (1) The obligations imposed on controllers or processors

2   under this Act do not restrict a controller's or processor's

3   ability to:

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

5   or regulations;

6   (b) comply with a civil, criminal, or regulatory

7   inquiry, investigation, subpoena, or summons by federal,

8   State, local, or other governmental authorities;

9   (c) cooperate with law enforcement agencies concerning

10   conduct or activity that the controller or processor

11   reasonably and in good faith believes may violate federal,

12   State, or local law;

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

14   (e) prevent or detect identity theft, fraud, or other

15   criminal activity or verify identities;

16   (f) perform a contract to which the consumer is a party

17   or in order to take steps at the request of the consumer

18   prior to entering into a contract;

19   (g) protect the vital interests of the consumer or of

20   another natural person;

21   (h) perform a task carried out in the public interest

22   or in the exercise of official authority vested in the

23   controller;

24   (i) process personal data of a consumer for one or more

25   specific purposes where the consumer has given their

26   consent to the processing; or

1   (j) prevent, detect, or respond to security incidents,

2   identity theft, fraud, harassment, malicious or deceptive

3   activities, or any illegal activity; preserve the

4   integrity or security of systems; or investigate, report,

5   or prosecute those responsible for any such action.

6   (2) The obligations imposed on controllers or processors

7   under this Act do not apply where compliance by the controller

8   or processor with this Act would violate an evidentiary

9   privilege under Illinois law and do not prevent a controller or

10   processor from providing personal data concerning a consumer to

11   a person covered by an evidentiary privilege under Illinois law

12   as part of a privileged communication.

13   (3) A controller or processor that discloses personal data

14   to a third-party controller or processor in compliance with the

15   requirements of this Act is not in violation of this Act,

16   including under Section 45, if the recipient processes such

17   personal data in violation of this Act, provided that, at the

18   time of disclosing the personal data, the disclosing controller

19   or processor did not have actual knowledge that the recipient

20   intended to commit a violation. A third-party controller or

21   processor receiving personal data from a controller or

22   processor is likewise not liable under this Act, including

23   under Section 45, for the obligations of a controller or

24   processor to which it provides services.

25   (4) This Act does not require a controller or processor to

26   do the following:

1   (a) Reidentify deidentified data.

2   (b) Retain, link, or combine personal data concerning a

3   consumer that it would not otherwise retain, link, or

4   combine in the ordinary course of business.

5   (c) Comply with a request to exercise any of the rights

6   under subsections (1) through (6) of Section 20 if the

7   controller is unable to verify, using commercially

8   reasonable efforts, the identity of the consumer making the

9   request.

10   (5) Obligations imposed on controllers and processors

11 under this Act do not:

12   (a) adversely affect the rights or freedoms of any

13   persons; or

14   (b) apply to the processing of personal data by a

15   natural person in the course of a purely personal or

16   household activity.

17   Section 45. Liability.

18   (1) This Act does not serve as the basis for a private

19 right of action under this Act or any other law.

20   (2) Where more than one controller or processor, or both a

21 controller and a processor, involved in the same processing, is

22 in violation of this Act, the liability shall be allocated

23 among the parties according to principles of comparative fault,

24 unless such liability is otherwise allocated by contract among

25 the parties.

1   Section 50. Enforcement.

2   (1) The General Assembly finds that the practices covered

3   by this Act are matters vitally affecting the public interest

4   for the purpose of applying the Consumer Fraud and Deceptive

5   Business Practices Act. A violation of this Act is not

6   reasonable in relation to the development and preservation of

7   business and is an unfair or deceptive act in trade or commerce

8   and an unfair method of competition for the purpose of applying

9   the Consumer Fraud and Deceptive Business Practices Act.

10   (2) The Attorney General may bring an action in the name of

11   the State, or as parens patriae on behalf of persons residing

12   in the State, to enforce this Act.

13   (3) A controller or processor is in violation of this Act

14   if it fails to cure any alleged violation of Sections 20

15   through 40 within 30 days after receiving notice of alleged

16   noncompliance. Any controller or processor that violates this

17   Act is subject to an injunction and liable for a civil penalty

18   of not more than $2,500 for each violation or $7,500 for each

19   intentional violation.

20   (4) The Consumer Privacy Fund is created as a special fund

21   in the State treasury. All receipts from the imposition of

22   civil penalties under this Act must be deposited into the Fund.

23   Moneys in the Fund may be spent only after appropriation.

24   Expenditures from the Fund may be used only to fund privacy and

25   data protection activities performed by the State Chief

1   Information Officer.

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

8   Section 90. The State Finance Act is amended by adding
9   Section 5.891 as follows:

10   (30 ILCS 105/5.891 new)
11   Sec. 5.891. The Consumer Privacy Fund.

12   Section 99. Effective date. This Act takes effect January
13   1, 2020.