



104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

SB3548

Introduced 2/5/2026, by Sen. Sue Rezin

SYNOPSIS AS INTRODUCED:

New Act
5 ILCS 140/7
30 ILCS 105/5.1038 new

Creates the Consumer Data Privacy Act. Establishes certain consumer rights relating to personal data, including the rights to confirm whether data is being processed, to correct any inaccuracies in the consumer's personal data, to delete personal data provided by the consumer, to obtain a copy of the consumer's personal data that was previously provided, and to opt out of targeted advertising, the sale of data, or profiling of the consumer. Defines terms. Applies to persons who conduct business in Illinois or produce products or services that are targeted to Illinois residents and that during the a calendar year control or process person data of at least 100,000 consumers or 25,0000 consumers and derives over 50% of gross revenue from the sale of personal data. Makes requirements for persons or entities that control and process consumer data and also exempts certain persons or entities from the statutory provisions of the Act. Provides that the Attorney General has exclusive authority to enforce the consumer data privacy rights. Creates the Consumer Privacy Fund to be administered by the Office of the Attorney General. Amends the Freedom of Information Act. Exempts from disclosure data protection impact assessments done under the Illinois Consumer Data Privacy Act. Makes a conforming change in the State Finance Act.

LRB104 18765 JRC 32208 b

1 AN ACT concerning civil law.

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
5 Consumer Data Privacy Act.

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

7 "Affiliate" means a legal entity that controls, is
8 controlled by, or is under common control with another legal
9 entity or shares common branding with another legal entity.
10 For the purposes of this definition, "control" or "controlled"
11 means:

12 (1) ownership of, or the power to vote, more than 50%
13 of the outstanding shares of any class of voting security
14 of a company;

15 (2) control in any manner over the election of a
16 majority of the directors or of individuals exercising
17 similar functions; or

18 (3) the power to exercise controlling influence over
19 the management of a company.

20 "Authenticate" means verifying through reasonable means
21 that the consumer entitled to exercise consumer rights granted
22 in Section 15 is the same consumer exercising consumer rights
23 with respect to the personal data at issue.

1 "Biometric data" means data generated by automatic
2 measurements of an individual's biological characteristics,
3 such as a fingerprint, voiceprint, eye retinas, irises, or
4 other unique biological patterns or characteristics that are
5 used to identify a specific individual. "Biometric data" does
6 not include a physical or digital photograph, a video or audio
7 recording, or data generated therefrom, unless that data is
8 generated to identify a specific individual or information
9 collected, used, or stored for health care treatment, payment,
10 or operations under HIPAA.

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

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

14 "Consent" means a clear affirmative act signifying a
15 consumer's freely given, specific, informed, and unambiguous
16 agreement to process personal data relating to the consumer.
17 "Consent" includes a written statement, written by electronic
18 means, or any other unambiguous affirmative action.

19 "Consumer" means a natural person who is a resident of the
20 State acting only in an individual context. "Consumer" does
21 not include a natural person acting in a commercial or
22 employment context.

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

26 "Covered entity" has the same meaning as in 45 CFR Sec.

1 160.103 under HIPAA.

2 "Decisions that produce legal or similarly significant
3 effects concerning a consumer" means a decision made by a
4 controller that results in the provision or denial by the
5 controller of financial and lending services, housing,
6 insurance, education enrollment, criminal justice, employment
7 opportunities, health care services, or access to basic
8 necessities like food and water.

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

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

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

19 "Health care provider" means:

20 (1) any health care facility as defined in Section
21 8-2001 of the Code of Civil Procedure;

22 (2) health care practitioner as defined in Section
23 8-2001 of the Code of Civil Procedure;

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

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

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

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

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

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

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

15 (3) provides an educational program for which it
16 awards a bachelor's or higher degree, or provides a
17 program that is acceptable for full credit toward such a
18 degree, a program of postgraduate or postdoctoral studies,
19 or a program of training to prepare students for gainful
20 employment in a recognized occupation; and

21 (4) is a public or other nonprofit institution.

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

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

26 (2) does not provide net earnings to, or operate in

1 any manner that inures to the benefit of, any officer,
2 employee, or shareholder of the entity.

3 "Personal data" means any information that is linked or
4 reasonably linkable to an identified or identifiable natural
5 person. "Personal data" does not include deidentified data or
6 publicly available information.

7 "Precise geolocation data" means information derived from
8 technology, including, but not limited to, global positioning
9 system level latitude and longitude coordinates or other
10 mechanisms, that directly identifies the specific location of
11 a natural person with precision and accuracy within a radius
12 of 1,750 feet. "Precise geolocation data" does not include the
13 content of communications, or any data generated by or
14 connected to advanced utility metering infrastructure systems
15 or equipment for use by a utility.

16 "Process" or "processing" means any operation or set of
17 operations performed, whether by manual or automated means, on
18 personal data or on sets of personal data, including, but not
19 limited to, the collection, use, storage, disclosure,
20 analysis, deletion, or modification of personal data.

21 "Processor" means a natural or legal entity that processes
22 personal data on behalf of a controller.

23 "Profiling" means any form of automated processing
24 performed on personal data to evaluate, analyze, or predict
25 personal aspects related to an identified or identifiable
26 natural person's economic situation, health, personal

1 preferences, interests, reliability, behavior, location, or
2 movements.

3 "Protected health information" has the same meaning as in
4 45 CFR Sec. 160.103 under HIPAA.

5 "Pseudonymous data" means personal data that cannot be
6 attributed to a specific natural person without the use of
7 additional information, as long as the additional information
8 is kept separately and is subject to appropriate technical and
9 organizational measures to ensure that the personal data is
10 not attributed to an identified or identifiable natural
11 person.

12 "Publicly available information" means information that is
13 lawfully made available through federal, State, or local
14 government records, or information that a business has a
15 reasonable basis to believe is lawfully made available to the
16 general public through widely distributed media, by the
17 consumer, or by a person to whom the consumer has disclosed the
18 information, unless the consumer has restricted the
19 information to a specific audience.

20 "Sale of personal data" means the exchange of personal
21 data for monetary consideration by the controller to a third
22 party. "Sale of personal data" does not include:

23 (1) the disclosure of personal data to a processor
24 that processes the personal data on behalf of the
25 controller;

26 (2) the disclosure of personal data to a third party

1 for purposes of providing a product or service requested
2 by the consumer;

3 (3) the disclosure or transfer of personal data to an
4 affiliate of the controller;

5 (4) the disclosure of information that the consumer
6 intentionally made available to the general public via a
7 channel of mass media and did not restrict to a specific
8 audience; or

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

14 "Sensitive data" means a category of personal data that
15 includes:

16 (1) personal data indicating racial or ethnic origin,
17 religious beliefs, mental or physical health diagnosis,
18 sexual orientation, or citizenship or immigration status;

19 (2) the processing of genetic or biometric data that
20 is processed for the purpose of uniquely identifying a
21 specific natural person;

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

23 (4) precise geolocation data.

24 "State agency" means:

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

1 State;

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

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

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

12 (1) advertisements based on activities within a
13 controller's own or affiliated websites or online
14 applications;

15 (2) advertisements based on the context of a
16 consumer's current search query, visit to a website, or
17 online application;

18 (3) advertisements directed to a consumer in response
19 to the consumer's request for information or feedback; or

20 (4) processing personal data solely for measuring or
21 reporting advertising performance, reach, or frequency.

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

26 "Trade secret" has the same meaning as in the Illinois

1 Trade Secrets Act.

2 Section 10. Coverage of act.

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

7 (1) 100,000 consumers; or

8 (2) 25,000 consumers and derive over 50% of gross
9 revenue from the sale of personal data.

10 (b) This Act does not apply to any:

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

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

15 (3) covered entity or business associate governed by
16 the privacy, security, and breach notification rules
17 issued by the United States Department of Health and Human
18 Services, 45 CFR Parts 160 and 164 established under
19 HIPAA;

20 (4) nonprofit organization;

21 (5) institution of higher education;

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

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

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

5 (1) protected health information under HIPAA;

6 (2) health records;

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

9 (4) identifiable private information for purposes of
10 the federal policy for the protection of human subjects
11 under 45 CFR Part 46; identifiable private information
12 that is otherwise information collected as part of human
13 subjects research under the good clinical practice
14 guidelines issued by the International Council for
15 Harmonisation of Technical Requirements for
16 Pharmaceuticals for Human Use; the protection of human
17 subjects under 21 CFR Parts 50 and 56, or personal data
18 used or shared in research conducted in accordance with
19 the requirements set forth in this Act, or other research
20 conducted in accordance with applicable law;

21 (5) information and documents created for purposes of
22 the federal Health Care Quality Improvement Act of 1986;

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

25 (7) information derived from any of the health
26 care-related information listed in this subsection that is

1 deidentified in accordance with the requirements for
2 deidentification under HIPAA;

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

9 (9) information used only for public health activities
10 and purposes as authorized by HIPAA;

11 (10) the collection, maintenance, disclosure, sale,
12 communication, or use of any personal information bearing
13 on a consumer's creditworthiness, credit standing, credit
14 capacity, character, general reputation, personal
15 characteristics, or mode of living by a consumer reporting
16 agency, furnisher, or user that provides information for
17 use in a consumer report, and by a user of a consumer
18 report, but only to the extent that the activity is
19 regulated by and authorized under the federal Fair Credit
20 Reporting Act;

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

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

26 (13) personal data collected, processed, sold, or

1 disclosed in compliance with the federal Farm Credit Act;

2 (14) data processed or maintained:

3 (A) in the course of an individual applying to,
4 employed by, or acting as an agent or independent
5 contractor of a controller, processor, or third party,
6 to the extent that the data is collected and used
7 within the context of that role;

8 (B) as the emergency contact information of an
9 individual used for emergency contact purposes; or

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

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

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

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

1 Section 15. Consumer rights and remedies.

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

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

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

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

18 (3) delete personal data provided by or obtained about
19 the consumer;

20 (4) obtain a copy of the consumer's personal data that
21 the consumer previously provided to the controller in a
22 portable and, to the extent technically practicable,
23 readily usable format that allows the consumer to transmit
24 the data to another controller without hindrance, if the
25 processing is carried out by automated means. The

1 controller may not be required to reveal any trade
2 secrets; and

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

8 (c) Except as otherwise provided in this Act, a controller
9 shall comply with a request by a consumer to exercise the
10 consumer rights under this Section as follows:

11 (1) a controller shall respond to the consumer without
12 undue delay, but in all cases within 45 days of receipt of
13 the request submitted under the methods described in this
14 Section. The response period may be extended once by 45
15 additional days if reasonably necessary, taking into
16 consideration the complexity and number of the consumer's
17 requests, as long as the controller informs the consumer
18 of any extension within the initial 45-day response
19 period, together with the reason for the extension;

20 (2) if a controller declines to take action regarding
21 the consumer's request, the controller shall inform the
22 consumer without undue delay, but no later than 45 days
23 after receipt of the request of the justification for
24 declining to take action and instructions on how to appeal
25 that decision;

26 (3) information provided in response to a consumer

1 request shall be provided by a controller free of charge,
2 up to twice annually per consumer. If requests from a
3 consumer are excessive, repetitive, technically
4 infeasible, or manifestly unfounded, the controller may
5 charge the consumer a reasonable fee to cover the
6 administrative costs of complying with the request or
7 decline to act on the request. The controller bears the
8 burden of demonstrating the excessive, repetitive,
9 technically infeasible, or manifestly unfounded nature of
10 the request;

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

18 (5) a controller that has obtained personal data about
19 a consumer from a source other than the consumer is deemed
20 in compliance with a consumer's request to delete such
21 data under this Section by:

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

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

4 (d) A controller shall establish a process for a consumer
5 to appeal the controller's refusal to take action on a request
6 within a reasonable period of time after the consumer's
7 receipt of the decision under of this Section. The appeal
8 process shall be conspicuously available and similar to the
9 process for submitting requests to initiate action under this
10 Section. Within 60 days of receipt of an appeal, a controller
11 shall inform the consumer in writing of any action taken or not
12 taken in response to the appeal, including a written
13 explanation of the reasons for the decisions. If the appeal is
14 denied, the controller shall also provide the consumer with an
15 online mechanism, if available, or other method through which
16 the consumer may contact the Attorney General to submit a
17 complaint.

18 Section 20. Controller's duties and responsibilities.

19 (a) A controller shall:

20 (1) limit the collection of personal data to what is
21 adequate, relevant, and reasonably necessary in relation
22 to the purposes for which the data is processed as
23 disclosed to the consumer;

24 (2) except as otherwise provided in this Section, not
25 process personal data for purposes that are neither

1 reasonably necessary to nor compatible with the disclosed
2 purposes for which the personal data is processed as
3 disclosed to the consumer, unless the controller obtains
4 the consumer's consent;

5 (3) establish, implement, and maintain reasonable
6 administrative, technical, and physical data security
7 practices to protect the confidentiality, integrity, and
8 accessibility of personal data. The data security
9 practices shall be appropriate to the volume and nature of
10 the personal data at issue;

11 (4) not process personal data in violation of State
12 and federal laws that prohibit unlawful discrimination
13 against consumers. A controller shall not discriminate
14 against a consumer for exercising any of the consumer
15 rights contained this Act, including denying goods or
16 services, charging different prices or rates for goods or
17 services, or providing a different level of quality of
18 goods and services to the consumer. Nothing in this
19 paragraph may be construed to require a controller to
20 provide a product or service that requires the personal
21 data of a consumer that the controller does not collect or
22 maintain or to prohibit a controller from offering a
23 different price, rate, level, quality, or selection of
24 goods or services to a consumer, including offering goods
25 or services for no fee, if the offer is related to a
26 consumer's voluntary participation in a bona fide loyalty,

1 rewards, premium features, discounts, or club card
2 program; and

3 (5) not process sensitive data concerning a consumer
4 without obtaining the consumer's consent, or, in the case
5 of the processing of sensitive data collected from a known
6 child, process the data in accordance with the federal
7 Children's Online Privacy Protection Act.

8 (b) Any provision of a contract or agreement of any kind
9 that purports to waive or limit in any way consumer rights
10 under this Act is deemed contrary to public policy and is void
11 and unenforceable.

12 (c) Controllers shall provide consumers with a reasonably
13 accessible, clear, and meaningful privacy notice that
14 includes:

15 (1) the categories of personal data processed by the
16 controller;

17 (2) the purpose for processing personal data;

18 (3) how consumers may exercise their consumer rights
19 under this Act, including how a consumer may appeal a
20 controller's decision regarding a consumer's request;

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

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

25 (d) If a controller sells personal data to third parties
26 or processes personal data for targeted advertising, the

1 controller shall clearly and conspicuously disclose such
2 activity, as well as the manner in which a consumer may
3 exercise the right to opt out of processing.

4 (e) A controller shall establish, and shall describe in a
5 privacy notice, one or more secure and reliable means for
6 consumers to submit a request to exercise their consumer
7 rights under this Act. The different ways to submit a request
8 by a consumer must consider the ways in which consumers
9 normally interact with the controller, the need for secure and
10 reliable communication of the requests, and the ability of the
11 controller to authenticate the identity of the consumer making
12 the request. Controllers may not require a consumer to create
13 a new account to exercise consumer rights under this Act but
14 may require a consumer to use an existing account.

15 Section 25. Processor duties and responsibilities.

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

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

24 (2) assisting the controller in meeting the
25 controller's obligations for the security of processing

1 the personal data and for the notification of a breach of
2 the security of the system of the processor under
3 applicable State law by taking into account the nature of
4 processing and the information available to the processor;
5 and

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

9 (b) A contract between a controller and a processor
10 governs the processor's data processing procedures for
11 processing performed on behalf of the controller. The contract
12 shall be binding and shall clearly set forth instructions for
13 processing personal data, the nature and purpose of
14 processing, the type of data subject to processing, the
15 duration of processing, and the rights and obligations of both
16 parties. The contract shall also include requirements that the
17 processor shall:

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

21 (2) at the controller's direction, delete or return
22 all personal data to the controller as requested at the
23 end of the provision of services, unless retention of the
24 personal data is required by law;

25 (3) upon the reasonable request of the controller,
26 make available to the controller all information in its

1 possession necessary to demonstrate the processor's
2 compliance with the obligations in this Act;

3 (4) allow and cooperate with reasonable assessments by
4 the controller or the controller's designated assessor.
5 Alternatively, the processor may arrange for a qualified
6 and independent assessor to conduct an assessment of the
7 processor's policies and technical and organizational
8 measures in support of the obligations in this Act using
9 an appropriate and accepted control standard or framework
10 and assessment procedure for assessments. The processor
11 shall provide a report of the assessment to the controller
12 upon request; and

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

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

20 (d) Determining whether a person is acting as a controller
21 or processor for a specific processing of data is a fact-based
22 determination that depends upon the context in which personal
23 data is to be processed. A processor that continues to adhere
24 to a controller's instructions for a specific processing of
25 personal data remains a processor.

1 Section 30. Required data protection impact assessment.

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

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

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

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

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

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

16 (C) a physical or other intrusion upon consumers'
17 solitude or seclusion or their private affairs or
18 concerns if an intrusion would be offensive to a
19 reasonable person; or

20 (D) other substantial injury to consumers;

21 (4) the processing of sensitive data; and

22 (5) any processing of personal data that presents a
23 heightened risk of harm to consumers.

24 (b) Data protection impact assessments conducted under
25 this Section shall identify and weigh the benefits that may
26 flow, directly and indirectly, from the processing, to the

1 controller, the consumer, other stakeholders, and the public
2 against the potential risks to the rights of the consumer
3 associated with such processing, as mitigated by safeguards
4 that can be employed by the controller to reduce the risk. The
5 use of deidentified data and the reasonable expectations of
6 consumers, as well as the context of the processing of
7 personal data and the relationship between the controller and
8 the consumer whose personal data will be processed, shall be
9 factored into this assessment by the controller.

10 (c) The Attorney General may request that a controller
11 disclose any data protection impact assessment that is
12 relevant to an investigation conducted by the Attorney
13 General, and the controller shall make the data protection
14 impact assessment available to the Attorney General. The
15 Attorney General may evaluate the data protection impact
16 assessments for compliance with the requirements of this Act.

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

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

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

1 activities.

2 (g) Data protection assessments conducted by a controller
3 for the purpose of compliance with other laws or regulations
4 may comply under this Section if the assessments have a
5 reasonably comparable scope and effect.

6 (h) Data protection assessment requirements apply to
7 processing activities created or generated on or after June 1,
8 2027.

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

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

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

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

18 (3) contractually obligate any recipients of the
19 deidentified data to comply with this Act.

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

22 (1) reidentify deidentified data or pseudonymous data;
23 or

24 (2) maintain data in identifiable form or collect,
25 obtain, retain, or access any data or technology to be

1 capable of associating an authenticated consumer request
2 with personal data.

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

6 (1) the controller is not reasonably capable of
7 associating the request with the personal data or it would
8 be unreasonably burdensome for the controller to associate
9 the request with the personal data;

10 (2) the controller does not use the personal data to
11 recognize or respond to the specific consumer who is the
12 subject of the personal data, or associate the personal
13 data with other personal data about the same specific
14 consumer; and

15 (3) the controller does not sell the personal data to
16 any third party or otherwise voluntarily disclose the
17 personal data to any third party other than a processor,
18 except as otherwise permitted in this Section.

19 (d) The consumer rights contained in this Act do not apply
20 to pseudonymous data in cases in which the controller is able
21 to demonstrate any information necessary to identify the
22 consumer is kept separately and is subject to appropriate
23 technical and organizational measures to ensure that the
24 personal data is not attributed to an identified or
25 identifiable natural person.

26 (e) A controller that discloses pseudonymous data or

1 de-identified data shall exercise reasonable oversight to
2 monitor compliance with any contractual commitments to which
3 the pseudonymous data or deidentified data is subject and take
4 appropriate steps to address any breaches of those contractual
5 commitments.

6 Section 40. Exceptions for controllers and processors.

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

9 (1) comply with federal, State, or local laws or
10 regulations;

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

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

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

20 (5) provide a product or service specifically
21 requested by a consumer or a parent or guardian of a known
22 child;

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

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

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

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

13 (10) engage in public or peer-reviewed scientific or
14 statistical research in the public interest that adheres
15 to all other applicable ethics and privacy laws and is
16 approved, monitored, and governed by an institutional
17 review board or similar independent oversight entities
18 that determine:

19 (A) if the deletion of the information is likely
20 to provide substantial benefits that do not
21 exclusively accrue to the controller;

22 (B) the expected benefits of the research outweigh
23 the privacy risks; and

24 (C) if the controller has implemented reasonable
25 safeguards to mitigate privacy risks associated with
26 research, including any risks associated with

1 reidentification; or

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

4 (b) The obligations imposed on controllers or processors
5 under this Act do not restrict a controller's or processor's
6 ability to collect, use, or retain data to:

7 (1) conduct internal research to develop, improve, or
8 repair products, services, or technology;

9 (2) effectuate a product recall;

10 (3) identify and repair technical errors that impair
11 existing or intended functionality; or

12 (4) perform internal operations that are reasonably
13 aligned with the expectations of the consumer or
14 reasonably anticipated based on the consumer's existing
15 relationship with the controller or are otherwise
16 compatible with processing data in furtherance of the
17 provision of a product or service specifically requested
18 by a consumer or a parent or guardian of a known child or
19 the performance of a contract to which the consumer or a
20 parent or guardian of a known child is a party.

21 (c) The obligations imposed on controllers or processors
22 under this Act do not apply to a controller or processor if
23 compliance would violate an evidentiary privilege under State
24 law. Nothing in this Act may be construed to prevent a
25 controller or processor from providing personal data
26 concerning a consumer to a person covered by an evidentiary

1 privilege under State laws as part of a privileged
2 communication.

3 (d) A controller or processor that discloses personal data
4 to a third-party controller or processor, in compliance with
5 the requirements of this Act, is not in violation of this Act
6 if the third-party controller or processor that receives and
7 processes such personal data is in violation of this Act;
8 provided that, at the time of disclosing the personal data,
9 the disclosing controller or processor did not have actual
10 knowledge that the recipient intended to commit a violation. A
11 third-party controller or processor receiving personal data
12 from a controller or processor in compliance with the
13 requirements of this Act is also not in violation of this Act
14 for the transgressions of the controller or processor from
15 which it receives such personal data.

16 (e) Nothing in this Act may be construed as an obligation
17 imposed on controllers and processors that adversely affects
18 the privacy or other rights or freedoms of any persons,
19 including, but not limited to, the right of free speech under
20 the First Amendment to the United States Constitution or
21 applies to the processing of personal data by a person in the
22 course of a purely personal or household activity.

23 (f) Personal data processed by a controller under this
24 Section may not be processed for any purpose other than those
25 expressly listed unless otherwise allowed by this Act.
26 Personal data processed by a controller under this Section may

1 be processed to the extent that such processing is:

2 (1) reasonably necessary and proportionate to the
3 purposes listed in this Section; and

4 (2) adequate, relevant, and limited to what is
5 necessary for the specific purposes listed in this
6 Section. Personal data collected, used, or retained under
7 this Section shall, if applicable, take into account the
8 nature and purpose or purposes of such collection, use, or
9 retention. The data shall be subject to reasonable
10 administrative, technical, and physical measures to
11 protect the confidentiality, integrity, and accessibility
12 of personal data and to reduce reasonably foreseeable
13 risks of harm to consumers relating to the collection,
14 use, or retention of personal data.

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

19 (h) Processing personal data for the purposes expressly
20 identified in this Section does not by itself make an entity a
21 controller with respect to such processing.

22 Section 45. Enforcement by the Attorney General.

23 (a) The Attorney General has exclusive authority to
24 enforce violations of this Act. The Attorney General may
25 enforce this Act by bringing an action in the name of the State

1 of Illinois on behalf of persons residing in this State. The
2 Attorney General has all powers and duties granted to the
3 Attorney General under State law to investigate and prosecute
4 any violation of this Act. The Attorney General may demand any
5 information, documents, or physical evidence from any
6 controller or processor believed to be engaged in, or about to
7 engage in, any violation of this Act.

8 (b) Before initiating any action for a violation of this
9 Act, the Attorney General shall provide a controller or
10 processor 30 days' written notice identifying the specific
11 provisions of this Act that the Attorney General alleges have
12 been or are being violated. If within the 30 days the
13 controller or processor cures the noticed violation and
14 provides the Attorney General an express written statement
15 that the alleged violations have been cured and that no
16 further violations will occur, no action for damages under
17 this Section may be initiated against the controller or
18 processor.

19 (c) If a controller or processor continues to violate this
20 Act following the cure period under this Section or breaches
21 an express written statement provided to the Attorney General
22 under this Section, the Attorney General may initiate an
23 action and seek damages for up to \$7,500 for each continued
24 violation under this Act.

25 (d) Nothing in this Act or any other law, regulation, or
26 the equivalent may be construed as providing the basis for, or

1 give rise to, a private right of action for violations of this
2 Act.

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

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

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

16 (5 ILCS 140/7)

17 (Text of Section before amendment by P.A. 104-300)

18 Sec. 7. Exemptions.

19 (1) When a request is made to inspect or copy a public
20 record that contains information that is exempt from
21 disclosure under this Section, but also contains information
22 that is not exempt from disclosure, the public body may elect
23 to redact the information that is exempt. The public body

1 shall make the remaining information available for inspection
2 and copying. Subject to this requirement, the following shall
3 be exempt from inspection and copying:

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

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

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

15 (c) Personal information contained within public
16 records, the disclosure of which would constitute a
17 clearly unwarranted invasion of personal privacy, unless
18 the disclosure is consented to in writing by the
19 individual subjects of the information. "Unwarranted
20 invasion of personal privacy" means the disclosure of
21 information that is highly personal or objectionable to a
22 reasonable person and in which the subject's right to
23 privacy outweighs any legitimate public interest in
24 obtaining the information. The disclosure of information
25 that bears on the public duties of public employees and
26 officials shall not be considered an invasion of personal

1 privacy.

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

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

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

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

17 (iv) unavoidably disclose the identity of a
18 confidential source, confidential information
19 furnished only by the confidential source, or persons
20 who file complaints with or provide information to
21 administrative, investigative, law enforcement, or
22 penal agencies; except that the identities of
23 witnesses to traffic crashes, traffic crash reports,
24 and rescue reports shall be provided by agencies of
25 local government, except when disclosure would
26 interfere with an active criminal investigation

1 conducted by the agency that is the recipient of the
2 request;

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

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

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

15 (d-5) A law enforcement record created for law
16 enforcement purposes and contained in a shared electronic
17 record management system if the law enforcement agency or
18 criminal justice agency that is the recipient of the
19 request did not create the record, did not participate in
20 or have a role in any of the events which are the subject
21 of the record, and only has access to the record through
22 the shared electronic record management system. As used in
23 this subsection (d-5), "criminal justice agency" means the
24 Illinois Criminal Justice Information Authority or the
25 Illinois Sentencing Policy Advisory Council.

26 (d-6) Records contained in the Officer Professional

1 Conduct Database under Section 9.2 of the Illinois Police
2 Training Act, except to the extent authorized under that
3 Section. This includes the documents supplied to the
4 Illinois Law Enforcement Training Standards Board from the
5 Illinois State Police and Illinois State Police Merit
6 Board.

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

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

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

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

24 (e-7) Records requested by persons committed to the
25 Department of Corrections or Department of Human Services
26 Division of Mental Health if those materials are available

1 through an administrative request to the Department of
2 Corrections or Department of Human Services Division of
3 Mental Health.

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

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

20 (e-10) Law enforcement records of other persons
21 requested by a person committed to the Department of
22 Corrections, Department of Human Services Division of
23 Mental Health, or a county jail, including, but not
24 limited to, arrest and booking records, mug shots, and
25 crime scene photographs, except as these records may be
26 relevant to the requester's current or potential case or

1 claim.

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

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

20 The information included under this exemption includes
21 all trade secrets and commercial or financial information
22 obtained by a public body, including a public pension
23 fund, from a private equity fund or a privately held
24 company within the investment portfolio of a private
25 equity fund as a result of either investing or evaluating
26 a potential investment of public funds in a private equity

1 fund. The exemption contained in this item does not apply
2 to the aggregate financial performance information of a
3 private equity fund, nor to the identity of the fund's
4 managers or general partners. The exemption contained in
5 this item does not apply to the identity of a privately
6 held company within the investment portfolio of a private
7 equity fund, unless the disclosure of the identity of a
8 privately held company may cause competitive harm.

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

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

20 (i) Valuable formulae, computer geographic systems,
21 designs, drawings, and research data obtained or produced
22 by any public body when disclosure could reasonably be
23 expected to produce private gain or public loss. The
24 exemption for "computer geographic systems" provided in
25 this paragraph (i) does not extend to requests made by
26 news media as defined in Section 2 of this Act when the

1 requested information is not otherwise exempt and the only
2 purpose of the request is to access and disseminate
3 information regarding the health, safety, welfare, or
4 legal rights of the general public.

5 (j) The following information pertaining to
6 educational matters:

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

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

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

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

20 (k) Architects' plans, engineers' technical
21 submissions, and other construction related technical
22 documents for projects not constructed or developed in
23 whole or in part with public funds and the same for
24 projects constructed or developed with public funds,
25 including, but not limited to, power generating and
26 distribution stations and other transmission and

1 distribution facilities, water treatment facilities,
2 airport facilities, sport stadiums, convention centers,
3 and all government owned, operated, or occupied buildings,
4 but only to the extent that disclosure would compromise
5 security.

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

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

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

22 (o) Administrative or technical information associated
23 with automated data processing operations, including, but
24 not limited to, software, operating protocols, computer
25 program abstracts, file layouts, source listings, object
26 modules, load modules, user guides, documentation

1 pertaining to all logical and physical design of
2 computerized systems, employee manuals, and any other
3 information that, if disclosed, would jeopardize the
4 security of the system or its data or the security of
5 materials exempt under this Section.

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

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

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

24 (s) Any and all proprietary information and records
25 related to the operation of an intergovernmental risk
26 management association or self-insurance pool or jointly

1 self-administered health and accident cooperative or pool.
2 Insurance or self-insurance (including any
3 intergovernmental risk management association or
4 self-insurance pool) claims, loss or risk management
5 information, records, data, advice, or communications.

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

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

18 (v) Vulnerability assessments, security measures, and
19 response policies or plans that are designed to identify,
20 prevent, or respond to potential attacks upon a
21 community's population or systems, facilities, or
22 installations, but only to the extent that disclosure
23 could reasonably be expected to expose the vulnerability
24 or jeopardize the effectiveness of the measures, policies,
25 or plans, or the safety of the personnel who implement
26 them or the public. Information exempt under this item may

1 include such things as details pertaining to the
2 mobilization or deployment of personnel or equipment, to
3 the operation of communication systems or protocols, to
4 cybersecurity vulnerabilities, or to tactical operations.

5 (w) (Blank).

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

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

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

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

26 (bb) Records and information provided to a mortality

1 review team and records maintained by a mortality review
2 team appointed under the Department of Juvenile Justice
3 Mortality Review Team Act.

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

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

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

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

24 (gg) Confidential information described in Section
25 1-100 of the Illinois Independent Tax Tribunal Act of
26 2012.

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

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

16 (jj) Confidential information described in Section
17 5-535 of the Civil Administrative Code of Illinois.

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

24 (ll) Records concerning the work of the threat
25 assessment team of a school district, including, but not
26 limited to, any threat assessment procedure under the

1 School Safety Drill Act and any information contained in
2 the procedure.

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

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

9 (oo) Records described in subsection (f) of Section
10 3-5-1 of the Unified Code of Corrections.

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

17 (qq) Reports described in subsection (e) of Section
18 16-15 of the Abortion Care Clinical Training Program Act.

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

21 (ss) For a request directed to a public body that is
22 also a HIPAA-covered entity, all information that is
23 protected health information, including demographic
24 information, that may be contained within or extracted
25 from any record held by the public body in compliance with
26 State and federal medical privacy laws and regulations,

1 including, but not limited to, the Health Insurance
2 Portability and Accountability Act and its regulations, 45
3 CFR Parts 160 and 164. As used in this paragraph,
4 "HIPAA-covered entity" has the meaning given to the term
5 "covered entity" in 45 CFR 160.103 and "protected health
6 information" has the meaning given to that term in 45 CFR
7 160.103.

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

12 (uu) Documents that, pursuant to the State of
13 Illinois' 1987 Agreement with the U.S. Nuclear Regulatory
14 Commission and the corresponding requirement to maintain
15 compatibility with the National Materials Program, have
16 been determined to be security sensitive. These documents
17 include information classified as safeguards,
18 safeguards-modified, and sensitive unclassified
19 nonsafeguards information, as identified in U.S. Nuclear
20 Regulatory Commission regulatory information summaries,
21 security advisories, and other applicable communications
22 or regulations related to the control and distribution of
23 security sensitive information.

24 (1.5) Any information exempt from disclosure under the
25 Judicial Privacy Act shall be redacted from public records
26 prior to disclosure under this Act.

1 (1.6) Any information exempt from disclosure under the
2 Public Official Safety and Privacy Act shall be redacted from
3 public records prior to disclosure under this Act.

4 (1.7) Any information exempt from disclosure under
5 paragraph (3.5) of Section 9-15 of the Election Code shall be
6 redacted from public records prior to disclosure under this
7 Act.

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

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

19 (Source: P.A. 103-154, eff. 6-30-23; 103-423, eff. 1-1-24;
20 103-446, eff. 8-4-23; 103-462, eff. 8-4-23; 103-540, eff.
21 1-1-24; 103-554, eff. 1-1-24; 103-605, eff. 7-1-24; 103-865,
22 eff. 1-1-25; 104-438, eff. 1-1-26; 104-443, eff. 1-1-26;
23 revised 1-7-26.)

24 (Text of Section after amendment by P.A. 104-300)

25 Sec. 7. Exemptions.

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

9 (a) Records created or compiled by a State public
10 defender agency or commission subject to the State Public
11 Defender Act that contain: individual client identity;
12 individual case file information; individual investigation
13 records and other records that are otherwise subject to
14 attorney-client privilege; records that would not be
15 discoverable in litigation; records under Section 2.15;
16 training materials; records related to attorney
17 consultation and representation strategy; or any of the
18 above concerning clients of county public defenders or
19 other defender agencies and firms. This exclusion does not
20 apply to deidentified, aggregated, administrative records,
21 such as general case processing and workload information.

22 (a-5) Information specifically prohibited from
23 disclosure by federal or State law or rules and
24 regulations implementing federal or State law.

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

1 or a court order.

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

7 (c) Personal information contained within public
8 records, the disclosure of which would constitute a
9 clearly unwarranted invasion of personal privacy, unless
10 the disclosure is consented to in writing by the
11 individual subjects of the information. "Unwarranted
12 invasion of personal privacy" means the disclosure of
13 information that is highly personal or objectionable to a
14 reasonable person and in which the subject's right to
15 privacy outweighs any legitimate public interest in
16 obtaining the information. The disclosure of information
17 that bears on the public duties of public employees and
18 officials shall not be considered an invasion of personal
19 privacy.

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

25 (i) interfere with pending or actually and
26 reasonably contemplated law enforcement proceedings

1 conducted by any law enforcement or correctional
2 agency that is the recipient of the request;

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

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

9 (iv) unavoidably disclose the identity of a
10 confidential source, confidential information
11 furnished only by the confidential source, or persons
12 who file complaints with or provide information to
13 administrative, investigative, law enforcement, or
14 penal agencies; except that the identities of
15 witnesses to traffic crashes, traffic crash reports,
16 and rescue reports shall be provided by agencies of
17 local government, except when disclosure would
18 interfere with an active criminal investigation
19 conducted by the agency that is the recipient of the
20 request;

21 (v) disclose unique or specialized investigative
22 techniques other than those generally used and known
23 or disclose internal documents of correctional
24 agencies related to detection, observation, or
25 investigation of incidents of crime or misconduct, and
26 disclosure would result in demonstrable harm to the

1 agency or public body that is the recipient of the
2 request;

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

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

7 (d-5) A law enforcement record created for law
8 enforcement purposes and contained in a shared electronic
9 record management system if the law enforcement agency or
10 criminal justice agency that is the recipient of the
11 request did not create the record, did not participate in
12 or have a role in any of the events which are the subject
13 of the record, and only has access to the record through
14 the shared electronic record management system. As used in
15 this subsection (d-5), "criminal justice agency" means the
16 Illinois Criminal Justice Information Authority or the
17 Illinois Sentencing Policy Advisory Council.

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

25 (d-7) Information gathered or records created from the
26 use of automatic license plate readers in connection with

1 Section 2-130 of the Illinois Vehicle Code.

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

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

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

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

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

1 institution or facility.

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

12 (e-10) Law enforcement records of other persons
13 requested by a person committed to the Department of
14 Corrections, Department of Human Services Division of
15 Mental Health, or a county jail, including, but not
16 limited to, arrest and booking records, mug shots, and
17 crime scene photographs, except as these records may be
18 relevant to the requester's current or potential case or
19 claim.

20 (f) Preliminary drafts, notes, recommendations,
21 memoranda, and other records in which opinions are
22 expressed, or policies or actions are formulated, except
23 that a specific record or relevant portion of a record
24 shall not be exempt when the record is publicly cited and
25 identified by the head of the public body. The exemption
26 provided in this paragraph (f) extends to all those

1 records of officers and agencies of the General Assembly
2 that pertain to the preparation of legislative documents.

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

12 The information included under this exemption includes
13 all trade secrets and commercial or financial information
14 obtained by a public body, including a public pension
15 fund, from a private equity fund or a privately held
16 company within the investment portfolio of a private
17 equity fund as a result of either investing or evaluating
18 a potential investment of public funds in a private equity
19 fund. The exemption contained in this item does not apply
20 to the aggregate financial performance information of a
21 private equity fund, nor to the identity of the fund's
22 managers or general partners. The exemption contained in
23 this item does not apply to the identity of a privately
24 held company within the investment portfolio of a private
25 equity fund, unless the disclosure of the identity of a
26 privately held company may cause competitive harm.

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

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

12 (i) Valuable formulae, computer geographic systems,
13 designs, drawings, and research data obtained or produced
14 by any public body when disclosure could reasonably be
15 expected to produce private gain or public loss. The
16 exemption for "computer geographic systems" provided in
17 this paragraph (i) does not extend to requests made by
18 news media as defined in Section 2 of this Act when the
19 requested information is not otherwise exempt and the only
20 purpose of the request is to access and disseminate
21 information regarding the health, safety, welfare, or
22 legal rights of the general public.

23 (j) The following information pertaining to
24 educational matters:

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

1 examination;

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

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

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

12 (k) Architects' plans, engineers' technical
13 submissions, and other construction related technical
14 documents for projects not constructed or developed in
15 whole or in part with public funds and the same for
16 projects constructed or developed with public funds,
17 including, but not limited to, power generating and
18 distribution stations and other transmission and
19 distribution facilities, water treatment facilities,
20 airport facilities, sport stadiums, convention centers,
21 and all government owned, operated, or occupied buildings,
22 but only to the extent that disclosure would compromise
23 security.

24 (l) Minutes of meetings of public bodies closed to the
25 public as provided in the Open Meetings Act until the
26 public body makes the minutes available to the public

1 under Section 2.06 of the Open Meetings Act.

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

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

14 (o) Administrative or technical information associated
15 with automated data processing operations, including, but
16 not limited to, software, operating protocols, computer
17 program abstracts, file layouts, source listings, object
18 modules, load modules, user guides, documentation
19 pertaining to all logical and physical design of
20 computerized systems, employee manuals, and any other
21 information that, if disclosed, would jeopardize the
22 security of the system or its data or the security of
23 materials exempt under this Section.

24 (p) Records relating to collective negotiating matters
25 between public bodies and their employees or
26 representatives, except that any final contract or

1 agreement shall be subject to inspection and copying.

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

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

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

24 (t) Information contained in or related to
25 examination, operating, or condition reports prepared by,
26 on behalf of, or for the use of a public body responsible

1 for the regulation or supervision of financial
2 institutions, insurance companies, or pharmacy benefit
3 managers, unless disclosure is otherwise required by State
4 law.

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

10 (v) Vulnerability assessments, security measures, and
11 response policies or plans that are designed to identify,
12 prevent, or respond to potential attacks upon a
13 community's population or systems, facilities, or
14 installations, but only to the extent that disclosure
15 could reasonably be expected to expose the vulnerability
16 or jeopardize the effectiveness of the measures, policies,
17 or plans, or the safety of the personnel who implement
18 them or the public. Information exempt under this item may
19 include such things as details pertaining to the
20 mobilization or deployment of personnel or equipment, to
21 the operation of communication systems or protocols, to
22 cybersecurity vulnerabilities, or to tactical operations.

23 (w) (Blank).

24 (x) Maps and other records regarding the location or
25 security of generation, transmission, distribution,
26 storage, gathering, treatment, or switching facilities

1 owned by a utility, by a power generator, or by the
2 Illinois Power Agency.

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

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

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

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

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

26 (dd) Correspondence and records (i) that may not be

1 disclosed under Section 11-9 of the Illinois Public Aid
2 Code or (ii) that pertain to appeals under Section 11-8 of
3 the Illinois Public Aid Code.

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

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

16 (gg) Confidential information described in Section
17 1-100 of the Illinois Independent Tax Tribunal Act of
18 2012.

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

23 (ii) Records requested by persons committed to or
24 detained by the Department of Human Services under the
25 Sexually Violent Persons Commitment Act or committed to
26 the Department of Corrections under the Sexually Dangerous

1 Persons Act if those materials: (i) are available in the
2 library of the facility where the individual is confined;
3 (ii) include records from staff members' personnel files,
4 staff rosters, or other staffing assignment information;
5 or (iii) are available through an administrative request
6 to the Department of Human Services or the Department of
7 Corrections.

8 (jj) Confidential information described in Section
9 5-535 of the Civil Administrative Code of Illinois.

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

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

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

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

1 (oo) Records described in subsection (f) of Section
2 3-5-1 of the Unified Code of Corrections.

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

9 (qq) Reports described in subsection (e) of Section
10 16-15 of the Abortion Care Clinical Training Program Act.

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

13 (ss) For a request directed to a public body that is
14 also a HIPAA-covered entity, all information that is
15 protected health information, including demographic
16 information, that may be contained within or extracted
17 from any record held by the public body in compliance with
18 State and federal medical privacy laws and regulations,
19 including, but not limited to, the Health Insurance
20 Portability and Accountability Act and its regulations, 45
21 CFR Parts 160 and 164. As used in this paragraph,
22 "HIPAA-covered entity" has the meaning given to the term
23 "covered entity" in 45 CFR 160.103 and "protected health
24 information" has the meaning given to that term in 45 CFR
25 160.103.

26 (tt) Proposals or bids submitted by engineering

1 consultants in response to requests for proposal or other
2 competitive bidding requests by the Department of
3 Transportation or the Illinois Toll Highway Authority.

4 (uu) Documents that, pursuant to the State of
5 Illinois' 1987 Agreement with the U.S. Nuclear Regulatory
6 Commission and the corresponding requirement to maintain
7 compatibility with the National Materials Program, have
8 been determined to be security sensitive. These documents
9 include information classified as safeguards,
10 safeguards-modified, and sensitive unclassified
11 nonsafeguards information, as identified in U.S. Nuclear
12 Regulatory Commission regulatory information summaries,
13 security advisories, and other applicable communications
14 or regulations related to the control and distribution of
15 security sensitive information.

16 (vv) Disclosure data protection impact assessments
17 done under the Consumer Data Privacy Act.

18 (1.5) Any information exempt from disclosure under the
19 Judicial Privacy Act shall be redacted from public records
20 prior to disclosure under this Act.

21 (1.6) Any information exempt from disclosure under the
22 Public Official Safety and Privacy Act shall be redacted from
23 public records prior to disclosure under this Act.

24 (1.7) Any information exempt from disclosure under
25 paragraph (3.5) of Section 9-15 of the Election Code shall be
26 redacted from public records prior to disclosure under this

1 Act.

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

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

13 (Source: P.A. 103-154, eff. 6-30-23; 103-423, eff. 1-1-24;
14 103-446, eff. 8-4-23; 103-462, eff. 8-4-23; 103-540, eff.
15 1-1-24; 103-554, eff. 1-1-24; 103-605, eff. 7-1-24; 103-865,
16 eff. 1-1-25; 104-300, eff. 1-1-27; 104-438, eff. 1-1-26;
17 104-443, eff. 1-1-26; revised 1-7-26.)

18 Section 905. The State Finance Act is amended by adding
19 Section 5.1038 as follows:

20 (30 ILCS 105/5.1038 new)

21 Sec. 5.1038. The Consumer Privacy Fund.

22 Section 995. No acceleration or delay. Where this Act
23 makes changes in a statute that is represented in this Act by

1 text that is not yet or no longer in effect (for example, a
2 Section represented by multiple versions), the use of that
3 text does not accelerate or delay the taking effect of (i) the
4 changes made by this Act or (ii) provisions derived from any
5 other Public Act.