



Sen. Sue Rezin

Filed: 3/24/2025

10400SB0052sam001

LRB104 03756 JRC 22863 a

1 AMENDMENT TO SENATE BILL 52

2 AMENDMENT NO. _____. Amend Senate Bill 52 by replacing
3 everything after the enacting clause with the following:

4 "Section 1. Short title. This Act may be cited as the
5 Illinois 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

1 similar functions; or

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

4 "Authenticate" means verifying through reasonable means
5 that the consumer entitled to exercise consumer rights granted
6 in Section 15 is the same consumer exercising consumer rights
7 with respect to the personal data at issue.

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

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

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

21 "Consent" means a clear affirmative act signifying a
22 consumer's freely given, specific, informed, and unambiguous
23 agreement to process personal data relating to the consumer.
24 "Consent" includes a written statement, written by electronic
25 means, or any other unambiguous affirmative action.

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

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

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

7 "Covered entity" has the same meaning as in 45 CFR Sec.
8 160.103 under HIPAA.

9 "Decisions that produce legal or similarly significant
10 effects concerning a consumer" means a decision made by a
11 controller that results in the provision or denial by the
12 controller of financial and lending services, housing,
13 insurance, education enrollment, criminal justice, employment
14 opportunities, health care services, or access to basic
15 necessities like food and water.

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

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

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

26 "Health care provider" means:

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

3 (2) health care practitioner as defined in Section
4 8-2001 of the Code of Civil Procedure;

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

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

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

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

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

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

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

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

1 employment in a recognized occupation; and

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

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

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

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

10 "Personal data" means any information that is linked or
11 reasonably linkable to an identified or identifiable natural
12 person. "Personal data" does not include deidentified data or
13 publicly available information.

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

23 "Process" or "processing" means any operation or set of
24 operations performed, whether by manual or automated means, on
25 personal data or on sets of personal data, including, but not
26 limited to, the collection, use, storage, disclosure,

1 analysis, deletion, or modification of personal data.

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

4 "Profiling" means any form of automated processing
5 performed on personal data to evaluate, analyze, or predict
6 personal aspects related to an identified or identifiable
7 natural person's economic situation, health, personal
8 preferences, interests, reliability, behavior, location, or
9 movements.

10 "Protected health information" has the same meaning as in
11 45 CFR Sec. 160.103 under HIPAA.

12 "Pseudonymous data" means personal data that cannot be
13 attributed to a specific natural person without the use of
14 additional information, as long as the additional information
15 is kept separately and is subject to appropriate technical and
16 organizational measures to ensure that the personal data is
17 not attributed to an identified or identifiable natural
18 person.

19 "Publicly available information" means information that is
20 lawfully made available through federal, State, or local
21 government records, or information that a business has a
22 reasonable basis to believe is lawfully made available to the
23 general public through widely distributed media, by the
24 consumer, or by a person to whom the consumer has disclosed the
25 information, unless the consumer has restricted the
26 information to a specific audience.

1 "Sale of personal data" means the exchange of personal
2 data for monetary consideration by the controller to a third
3 party. "Sale of personal data" does not include:

4 (1) the disclosure of personal data to a processor
5 that processes the personal data on behalf of the
6 controller;

7 (2) the disclosure of personal data to a third party
8 for purposes of providing a product or service requested
9 by the consumer;

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

12 (4) the disclosure of information that the consumer
13 intentionally made available to the general public via a
14 channel of mass media and did not restrict to a specific
15 audience; or

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

21 "Sensitive data" means a category of personal data that
22 includes:

23 (1) personal data indicating racial or ethnic origin,
24 religious beliefs, mental or physical health diagnosis,
25 sexual orientation, or citizenship or immigration status;

26 (2) the processing of genetic or biometric data that

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

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

4 (4) precise geolocation data.

5 "State agency" means:

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

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

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

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

19 (1) advertisements based on activities within a
20 controller's own or affiliated websites or online
21 applications;

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

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

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

3 "Third party" means a natural or legal person, public
4 authority, agency, or body other than the consumer,
5 controller, processor, or an affiliate of the processor or the
6 controller.

7 "Trade secret" has the same meaning as in the Illinois
8 Trade Secrets Act.

9 Section 10. Coverage of act.

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

14 (1) 100,000 consumers; or

15 (2) 25,000 consumers and derive over 50% of gross
16 revenue from the sale of personal data.

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

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

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

22 (3) covered entity or business associate governed by
23 the privacy, security, and breach notification rules
24 issued by the United States Department of Health and Human
25 Services, 45 CFR Parts 160 and 164 established under

1 HIPAA;

2 (4) nonprofit organization;

3 (5) institution of higher education;

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

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

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

12 (1) protected health information under HIPAA;

13 (2) health records;

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

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

1 conducted in accordance with applicable law;

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

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

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

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

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

18 (10) the collection, maintenance, disclosure, sale,
19 communication, or use of any personal information bearing
20 on a consumer's creditworthiness, credit standing, credit
21 capacity, character, general reputation, personal
22 characteristics, or mode of living by a consumer reporting
23 agency, furnisher, or user that provides information for
24 use in a consumer report, and by a user of a consumer
25 report, but only to the extent that the activity is
26 regulated by and authorized under the federal Fair Credit

1 Reporting Act;

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

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

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

9 (14) data processed or maintained:

10 (A) in the course of an individual applying to,
11 employed by, or acting as an agent or independent
12 contractor of a controller, processor, or third party,
13 to the extent that the data is collected and used
14 within the context of that role;

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

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

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

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

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

8 Section 15. Consumer rights and remedies.

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

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

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

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

25 (3) delete personal data provided by or obtained about

1 the consumer;

2 (4) obtain a copy of the consumer's personal data that
3 the consumer previously provided to the controller in a
4 portable and, to the extent technically practicable,
5 readily usable format that allows the consumer to transmit
6 the data to another controller without hindrance, if the
7 processing is carried out by automated means. The
8 controller may not be required to reveal any trade
9 secrets; and

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

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

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

1 (2) if a controller declines to take action regarding
2 the consumer's request, the controller shall inform the
3 consumer without undue delay, but no later than 45 days
4 after receipt of the request of the justification for
5 declining to take action and instructions on how to appeal
6 that decision;

7 (3) information provided in response to a consumer
8 request shall be provided by a controller free of charge,
9 up to twice annually per consumer. If requests from a
10 consumer are excessive, repetitive, technically
11 infeasible, or manifestly unfounded, the controller may
12 charge the consumer a reasonable fee to cover the
13 administrative costs of complying with the request or
14 decline to act on the request. The controller bears the
15 burden of demonstrating the excessive, repetitive,
16 technically infeasible, or manifestly unfounded nature of
17 the request;

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

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

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

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

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

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

25 Section 20. Controller's duties and responsibilities.

1 (a) A controller shall:

2 (1) limit the collection of personal data to what is
3 adequate, relevant, and reasonably necessary in relation
4 to the purposes for which the data is processed as
5 disclosed to the consumer;

6 (2) except as otherwise provided in this Section, not
7 process personal data for purposes that are neither
8 reasonably necessary to nor compatible with the disclosed
9 purposes for which the personal data is processed as
10 disclosed to the consumer, unless the controller obtains
11 the consumer's consent;

12 (3) establish, implement, and maintain reasonable
13 administrative, technical, and physical data security
14 practices to protect the confidentiality, integrity, and
15 accessibility of personal data. The data security
16 practices shall be appropriate to the volume and nature of
17 the personal data at issue;

18 (4) not process personal data in violation of State
19 and federal laws that prohibit unlawful discrimination
20 against consumers. A controller shall not discriminate
21 against a consumer for exercising any of the consumer
22 rights contained this Act, including denying goods or
23 services, charging different prices or rates for goods or
24 services, or providing a different level of quality of
25 goods and services to the consumer. Nothing in this
26 paragraph may be construed to require a controller to

1 provide a product or service that requires the personal
2 data of a consumer that the controller does not collect or
3 maintain or to prohibit a controller from offering a
4 different price, rate, level, quality, or selection of
5 goods or services to a consumer, including offering goods
6 or services for no fee, if the offer is related to a
7 consumer's voluntary participation in a bona fide loyalty,
8 rewards, premium features, discounts, or club card
9 program; and

10 (5) not process sensitive data concerning a consumer
11 without obtaining the consumer's consent, or, in the case
12 of the processing of sensitive data collected from a known
13 child, process the data in accordance with the federal
14 Children's Online Privacy Protection Act.

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

19 (c) Controllers shall provide consumers with a reasonably
20 accessible, clear, and meaningful privacy notice that
21 includes:

22 (1) the categories of personal data processed by the
23 controller;

24 (2) the purpose for processing personal data;

25 (3) how consumers may exercise their consumer rights
26 under this Act, including how a consumer may appeal a

1 controller's decision regarding a consumer's request;

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

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

6 (d) If a controller sells personal data to third parties
7 or processes personal data for targeted advertising, the
8 controller shall clearly and conspicuously disclose such
9 activity, as well as the manner in which a consumer may
10 exercise the right to opt out of processing.

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

22 Section 25. Processor duties and responsibilities.

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

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

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

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

16 (b) A contract between a controller and a processor
17 governs the processor's data processing procedures for
18 processing performed on behalf of the controller. The contract
19 shall be binding and shall clearly set forth instructions for
20 processing personal data, the nature and purpose of
21 processing, the type of data subject to processing, the
22 duration of processing, and the rights and obligations of both
23 parties. The contract shall also include requirements that the
24 processor shall:

25 (1) ensure that each person processing personal data
26 is subject to a duty of confidentiality with respect to

1 the data;

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

6 (3) upon the reasonable request of the controller,
7 make available to the controller all information in its
8 possession necessary to demonstrate the processor's
9 compliance with the obligations in this Act;

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

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

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

1 (d) Determining whether a person is acting as a controller
2 or processor for a specific processing of data is a fact-based
3 determination that depends upon the context in which personal
4 data is to be processed. A processor that continues to adhere
5 to a controller's instructions for a specific processing of
6 personal data remains a processor.

7 Section 30. Required data protection impact assessment.

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

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

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

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

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

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

22 (C) a physical or other intrusion upon consumers'
23 solitude or seclusion or their private affairs or
24 concerns if an intrusion would be offensive to a
25 reasonable person; or

1 (D) other substantial injury to consumers;

2 (4) the processing of sensitive data; and

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

5 (b) Data protection impact assessments conducted under
6 this Section shall identify and weigh the benefits that may
7 flow, directly and indirectly, from the processing, to the
8 controller, the consumer, other stakeholders, and the public
9 against the potential risks to the rights of the consumer
10 associated with such processing, as mitigated by safeguards
11 that can be employed by the controller to reduce the risk. The
12 use of deidentified data and the reasonable expectations of
13 consumers, as well as the context of the processing of
14 personal data and the relationship between the controller and
15 the consumer whose personal data will be processed, shall be
16 factored into this assessment by the controller.

17 (c) The Attorney General may request that a controller
18 disclose any data protection impact assessment that is
19 relevant to an investigation conducted by the Attorney
20 General, and the controller shall make the data protection
21 impact assessment available to the Attorney General. The
22 Attorney General may evaluate the data protection impact
23 assessments for compliance with the requirements of this Act.

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

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

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

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

13 (h) Data protection assessment requirements apply to
14 processing activities created or generated on or after June 1,
15 2027.

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

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

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

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

25 (3) contractually obligate any recipients of the

1 deidentified data to comply with this Act.

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

4 (1) reidentify deidentified data or pseudonymous data;

5 or

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

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

13 (1) the controller is not reasonably capable of
14 associating the request with the personal data or it would
15 be unreasonably burdensome for the controller to associate
16 the request with the personal data;

17 (2) the controller does not use the personal data to
18 recognize or respond to the specific consumer who is the
19 subject of the personal data, or associate the personal
20 data with other personal data about the same specific
21 consumer; and

22 (3) the controller does not sell the personal data to
23 any third party or otherwise voluntarily disclose the
24 personal data to any third party other than a processor,
25 except as otherwise permitted in this Section.

26 (d) The consumer rights contained in this Act do not apply

1 to pseudonymous data in cases in which the controller is able
2 to demonstrate any information necessary to identify the
3 consumer is kept separately and is subject to appropriate
4 technical and organizational measures to ensure that the
5 personal data is not attributed to an identified or
6 identifiable natural person.

7 (e) A controller that discloses pseudonymous data or
8 de-identified data shall exercise reasonable oversight to
9 monitor compliance with any contractual commitments to which
10 the pseudonymous data or deidentified data is subject and take
11 appropriate steps to address any breaches of those contractual
12 commitments.

13 Section 40. Exceptions for controllers and processors.

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

16 (1) comply with federal, State, or local laws or
17 regulations;

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

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

25 (4) investigate, establish, exercise, prepare for, or

1 defend legal claims;

2 (5) provide a product or service specifically
3 requested by a consumer or a parent or guardian of a known
4 child;

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

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

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

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

20 (10) engage in public or peer-reviewed scientific or
21 statistical research in the public interest that adheres
22 to all other applicable ethics and privacy laws and is
23 approved, monitored, and governed by an institutional
24 review board or similar independent oversight entities
25 that determine:

26 (A) if the deletion of the information is likely

1 to provide substantial benefits that do not
2 exclusively accrue to the controller;

3 (B) the expected benefits of the research outweigh
4 the privacy risks; and

5 (C) if the controller has implemented reasonable
6 safeguards to mitigate privacy risks associated with
7 research, including any risks associated with
8 reidentification; or

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

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

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

16 (2) effectuate a product recall;

17 (3) identify and repair technical errors that impair
18 existing or intended functionality; or

19 (4) perform internal operations that are reasonably
20 aligned with the expectations of the consumer or
21 reasonably anticipated based on the consumer's existing
22 relationship with the controller or are otherwise
23 compatible with processing data in furtherance of the
24 provision of a product or service specifically requested
25 by a consumer or a parent or guardian of a known child or
26 the performance of a contract to which the consumer or a

1 parent or guardian of a known child is a party.

2 (c) The obligations imposed on controllers or processors
3 under this Act do not apply to a controller or processor if
4 compliance would violate an evidentiary privilege under State
5 law. Nothing in this Act may be construed to prevent a
6 controller or processor from providing personal data
7 concerning a consumer to a person covered by an evidentiary
8 privilege under State laws as part of a privileged
9 communication.

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

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

1 the First Amendment to the United States Constitution or
2 applies to the processing of personal data by a person in the
3 course of a purely personal or household activity.

4 (f) Personal data processed by a controller under this
5 Section may not be processed for any purpose other than those
6 expressly listed unless otherwise allowed by this Act.
7 Personal data processed by a controller under this Section may
8 be processed to the extent that such processing is:

9 (1) reasonably necessary and proportionate to the
10 purposes listed in this Section; and

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

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

26 (h) Processing personal data for the purposes expressly

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

3 Section 45. Enforcement by the Attorney General.

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

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

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

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

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

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

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

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

23 (5 ILCS 140/7)

1 Sec. 7. Exemptions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 (j) The following information pertaining to
9 educational matters:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 (w) (Blank).

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

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

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

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

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

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

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

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

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

1 (gg) Confidential information described in Section
2 1-100 of the Illinois Independent Tax Tribunal Act of
3 2012.

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

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

19 (jj) Confidential information described in Section
20 5-535 of the Civil Administrative Code of Illinois.

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

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

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

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

12 (oo) Records described in subsection (f) of Section
13 3-5-1 of the Unified Code of Corrections.

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

20 (qq) Reports described in subsection (e) of Section
21 16-15 of the Abortion Care Clinical Training Program Act.

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

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

1 information, that may be contained within or extracted
2 from any record held by the public body in compliance with
3 State and federal medical privacy laws and regulations,
4 including, but not limited to, the Health Insurance
5 Portability and Accountability Act and its regulations, 45
6 CFR Parts 160 and 164. As used in this paragraph,
7 "HIPAA-covered entity" has the meaning given to the term
8 "covered entity" in 45 CFR 160.103 and "protected health
9 information" has the meaning given to that term in 45 CFR
10 160.103.

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

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

17 (1.5) Any information exempt from disclosure under the
18 Judicial Privacy Act shall be redacted from public records
19 prior to disclosure under this Act.

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

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

5 (Source: P.A. 102-38, eff. 6-25-21; 102-558, eff. 8-20-21;
6 102-694, eff. 1-7-22; 102-752, eff. 5-6-22; 102-753, eff.
7 1-1-23; 102-776, eff. 1-1-23; 102-791, eff. 5-13-22; 102-982,
8 eff. 7-1-23; 102-1055, eff. 6-10-22; 103-154, eff. 6-30-23;
9 103-423, eff. 1-1-24; 103-446, eff. 8-4-23; 103-462, eff.
10 8-4-23; 103-540, eff. 1-1-24; 103-554, eff. 1-1-24; 103-605,
11 eff. 7-1-24; 103-865, eff. 1-1-25.)

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

14 (30 ILCS 105/5.1030 new)

15 Sec. 5.1030. The Consumer Privacy Fund."