SYNOPSIS AS INTRODUCED:

New Act

Creates the Data Transparency and Privacy Act. Provides that any business that processes personal information or deidentified information must, prior to processing, provide notice to the consumer to whom the information refers or belongs of specific information in the service agreement or somewhere readily accessible on the business' website or mobile application. Establishes a "right to know" for consumers and prescribes types of information that they may request of businesses. Provides that consumers have the right to opt out of agreements that entail the disclosure of personal information from the business to third parties and affiliates, the sale of personal information from the business to third parties and affiliates, and the processing of personal information by the business, third parties, and affiliates. Provides that consumers have the right to request that a business correct inaccurate personal information about the consumer or delete personal information about the consumer. Prescribes a protocol for the handling of consumer requests by businesses. Prescribes pricing incentives and prohibitions against discrimination. Provides that businesses, affiliates, and third parties must conduct risk assessments and provides requirements for the assessments. Provides that enforcement of the Act may arise through private actions or enforcement by the Attorney General. Provides that any waiver of the provisions of the Act is void and unenforceable. Contains home rule preemption and severability provisions. Effective July 1, 2021.
AN ACT concerning business.

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

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

Section 5. Findings. The General Assembly finds and declares that:

(1) The right to privacy is a personal and fundamental right protected by the United States Constitution. As such, all individuals have a right to privacy and a personal property interest in information pertaining to them and that information shall be adequately protected from unlawful invasions and takings. This State recognizes the importance of providing consumers with transparency about how their personal information is stored, used, and shared by businesses. This transparency is crucial for Illinois citizens to protect themselves and their families from cyber-crimes and identity thieves.

(2) Businesses are now collecting, sharing, and selling personal information in ways not contemplated or properly covered by current law.

(a) Some websites install tracking tools that record when consumers visit web pages and send personal
information collected to third party marketers and data brokers.

(b) Third-party data broker companies are buying, selling, and trading personal information obtained from mobile phones, financial institutions, social media sites, and other online and brick and mortar companies.

(c) Social media companies, credit agencies and retail stores have all had their internal security systems breached, resulting in consumers' personal information being stolen and sold on the black market.

(3) Illinois consumers must be better informed about what kinds of personal information are collected, how information is shared with third parties, and how businesses store consumers' personal information. With this specific information, consumers can knowledgeably choose to opt in, opt out, or choose among businesses that disclose information to third parties on the basis of how protective the business is of consumers' privacy in order to properly protect their privacy, property, personal safety, and financial security.

Section 10. Definitions. As used in this Act:

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity.
"Business" means any sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that does business in the State of Illinois and meets one or more of the following thresholds:

(1) The business collects or discloses the personal information of 50,000 or more persons, Illinois households, or the combination thereof.

(2) The business derives 50% or more of its annual revenues from selling consumers' personal information.

"Business" does not include any third party that operates, hosts, or manages, but does not own, a website or online service on the owner's behalf or by processing information on behalf of the owners, or any State and local governments or municipal corporations.

"Categories of sources" means types of entities from which a business collects personal information about consumers, including, but not limited to, the consumer directly, government entities from which public records are obtained, and consumer data resellers.

"Categories of third parties" means types of entities that do not collect personal information directly from consumers, including, but not limited to, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks,
and consumer data resellers.

"Consumer" means a natural person residing in this State. "Consumer" does not include a natural person acting in an employment context.

"Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

1. Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2. Has implemented business processes that specifically prohibit reidentification of the information.
3. Has implemented business processes to prevent inadvertent release of deidentified information.
4. Makes no attempt to reidentify the information.

"Designated request address" means an electronic mail address, online form, mailing address, or toll-free telephone number that a consumer may use to request information, opt out of the sale or disclosure of personal information, or correct or delete personal information, as required to be provided under this Act.

"Disclose" means to disclose, release, transfer, share, disseminate, make available, or otherwise communicate orally, in writing, or by electronic or any other means a consumer's
personal information to any affiliate or third party.

"Disclose" does not include:

(1) Disclosure of personal information by a business to a third party or service provider under a written contract authorizing the third party or service provider to use the personal information to perform services on behalf of the business, including, but not limited to, maintaining or servicing accounts, disclosure of personal information by a business to a service provider, processing or fulfilling orders and transactions, verifying consumer information, processing payments, providing financing, or similar services, but only if: the contract prohibits the third party or service provider from using the personal information for any reason other than performing the specified service on behalf of the business and from disclosing any such personal information to additional third parties or service providers unless those additional third parties or service providers are allowed by the contract to further the specified services and the additional third parties and service providers and subject to the same restrictions imposed by this subsection.

(2) Disclosure of personal information by a business to a third party based on a good faith belief that disclosure is required to comply with applicable law, regulation, legal process, or court order.

(3) Disclosure of personal information by a business to
a third party that is reasonably necessary to address fraud, risk management, security, or technical issues; to protect the disclosing business' right or property; or to protect consumers or the public from illegal activities.

(4) Disclosure of personal information by a business to a third party in connection with the proposed or actual sale, merger, or bankruptcy of the business, to a third party.

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

(1) Identifiers such as a real name, alias, signature, postal address, telephone number, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, state identification number, passport number, physical characteristics or description, insurance policy number, employment, employment history, bank account number, credit card number, debit card number, financial information, medical information, health insurance information, or other similar identifiers.

(2) Characteristics of protected classifications under Illinois or federal law.

(3) Commercial information, including records of
personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(4) Biometric information.

(5) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application or advertisement.

(6) Geolocation data.

(7) Audio, electronic, visual, thermal, olfactory, or similar information.

(8) Professional or employment-related information.

(9) Educational information.

(10) Inferences drawn from any of the information identified in this Section to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

"Personal information" does not include publicly available information which the business obtained directly from records lawfully made available from federal, state, or local government records. "Personal information" does not include consumer information that is deidentified or aggregate consumer information.
"Process" or "processes" means any collection, use, storage, disclosure, analysis, deletion, or modification of personal information.

"Request" means a consumer right set forth in this Act including one or more of the following: (i) for the disclosure of information regarding a consumer's personal information; (ii) the opt out of sale or disclosure of a consumer's personal information; (iii) the correction of inaccurate personal information; and (iv) the deletion of personal information.

"Sale" or "sell" means the selling, renting, or licensing of a consumer's personal information by a business to a third party in direct exchange for monetary consideration, whereby, as a result of such transaction, the third party may use the personal information for its own commercial purposes. "Sale" or "sell" does not include circumstances in which:

(1) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party or affiliate, provided the third party or affiliate does not also sell the personal information, unless that disclosure would be consistent with the provisions of this Act. An intentional interaction occurs when the consumer intends to interact with the third party by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.
(2) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of altering third parties or affiliates that the consumer has opted out of the sale of the consumer's personal information.

(3) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose or business purposes if the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purposes.

(4) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party or affiliate assumes control of all or part of the business, provided that information is used or shared consistently with this Act. If a third party or affiliate materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistent with Section 20 and Section 25. This subparagraph does not authorize a business to make material, retroactive privacy
policy changes or make other changes in their privacy policy in a manner that would violate the Consumer Fraud and Deceptive Business Practices Act.

(5) A business uses a consumer's personal information to sell targeted advertising space to a third party as long as the personal information is not sold by the business to the third party or affiliate.

(6) The disclosure or transfer of personal information to an affiliate of the business.

"Service provider" means the natural or legal person that processes personal information on behalf of the business.

"Third party" means a business that is: (1) not an affiliate of the business that has collected, disclosed, or sold personal information; or (2) an affiliate with the business that has collected, disclosed, or sold personal information and the affiliate relationship is not clear to the consumer.

Section 15. Right to transparency. Any business that processes personal information or deidentified information must, prior to processing, provide notice to the consumer of the following in the service agreement or somewhere readily accessible on the business' website or mobile application:

(1) All categories of personal information and deidentified information that the business processes about individual consumers;
(2) All categories of third parties and affiliates with whom the business may disclose or sell that personal information or deidentified information and the business purpose for the disclosure or sale;

(3) The process in which an individual consumer may:
   (A) review the personal information collected by the business;
   (B) request changes to inaccurate personal information;
   (C) opt out of the disclosure or sale of personal information; and
   (D) request deletion of personal information; and

(4) The process in which the business notifies consumers of material changes to the notice required to be made available under this Section.

Section 20. Right to know. Consumers may request the following information of businesses:

(1) Copies of specific pieces of personal information about the consumer processed by the business.

(2) Categories of sources for the personal information processed.

(3) Name and contact information for each third party and affiliate to whom the personal information is disclosed or sold.
Section 25. Right to opt out, correct, and delete.
Consumers have the following rights concerning their personal information:

(1) The right to request to opt out of the following:
   (A) the disclosure of personal information from the business to third parties and affiliates;
   (B) the sale of personal information from the business to third parties and affiliates; and
   (C) the processing of personal information by the business, third parties, and affiliates.

(2) The right to request that a business correct inaccurate personal information about the consumer.

(3) The right to request that a business delete personal information about the consumer.

Section 30. Consumer requests and business responses.
(a) Businesses shall establish a process for collecting consumer requests and reasonably authenticating consumers making the requests and reasonably authenticating any request to correct inaccurate personal information. The method by which a consumer may submit a request under Section 20 and Section 25 shall be done in a form and manner determined by the business in a way that is not overly burdensome on the consumer.

(b) A business shall post on its website, online service, and within any mobile application, a link to a designated request address web page maintained by the business for the
The purpose of collecting and processing consumer requests. The business shall also post a designated request street address for consumers to submit requests by mail.

(c) A parent or legal guardian of a consumer under the age of 13 may submit a request on behalf of that consumer.

(d) A business that receives a request from a consumer through a designated request address shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required or confirmation of the consumer's opt out, correction or deletion request and business' compliance.

(1) The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily usable format that allows the consumer to transmit this information to another entity without hindrance.

(2) A business that has received a request to opt out of the disclosure or sale of a consumer's personal information shall be prohibited from selling or disclosing that consumer's personal information after its receipt of the consumer's request, unless the consumer subsequently provides express authorization for the sale or disclosure of the consumer's personal information.

(3) A business that receives a request to delete the consumer's personal information, shall delete the
consumer's personal information from its records and
direct any third party or affiliate with whom the personal
information was disclosed, to delete the consumer's
personal information from their records.

(4) A business shall not be required to comply with a
consumer's request to delete the consumer's personal
information if it is necessary for the business to maintain
the consumer's personal information in order to:

(i) Complete the transaction for which the
personal information was collected, provide a good or
service requested by the consumer, or reasonably
anticipated within the context of a business' ongoing
business relationship with the consumer, or otherwise
perform a contract between the business and the
consumer.

(ii) Detect security incidents, protect against
malicious, deceptive, fraudulent, or illegal activity;
or prosecute those responsible for that activity.

(iii) Debug to identify and repair errors that
impair existing intended functionality.

(iv) Exercise free speech, ensure the right of
another consumer to exercise their right of free
speech, or exercise another right provided for by law.

(v) Engage in public or peer-reviewed scientific,
historical, or statistical research in the public
interest that adheres to all other applicable ethics
and privacy laws, when the business' deletion of the
information is likely to render impossible or
seriously impair the achievement of such research, if
the consumer has provided informed consent.

(vi) To enable solely internal uses that are
reasonably aligned with the expectations of the
consumer based on the consumer's relationship with the
business.

(vii) Comply with a legal obligation.

(viii) Otherwise use the consumer's personal
information, internally, in a lawful manner that is
compatible with the context in which the consumer
provided the information.

(e) A business must provide a response to the consumer
within 45 days of a request under Section 20 and Section 25.

(1) The business shall promptly take steps to verify
the request, but shall not extend the business' duty to
disclose and deliver the information within 45 days of
receipt of the consumer's request. The time period to
provide the required information may be extended once by an
additional 45 days when reasonably necessary, provided the
consumer is provided notice of the extension within the
first 45-day period.

(2) The disclosure shall cover at least the 12-month
period preceding the business' receipt of the request. The
business shall not require the consumer to create an
account with the business in order to make a request.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any consumer request is manifestly unfounded or excessive.

(f) A business shall not be required to respond to a request made by or on behalf of the same consumer more than once in any 12-month period.

Section 35. Businesses, affiliates, and third parties.

(a) A business is not required to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(b) A business shall not reidentify any deidentified consumer information, unless the consumer subsequently provides express authorization for reidentification of deidentified information.

(c) A business shall not sell the personal information of
any consumer for which the business has actual knowledge that
the consumer is less than 16 years of age. A business that
willfully disregards the consumer's age shall be deemed to have
had actual knowledge of the consumer's age.

(d) A business shall not use a consumer's personal
information for any purpose other than those disclosed in the
notice at collection. If the business intends to use a
consumer's personal information for a purpose that was not
previously disclosed to the consumer in the notice at
collection, the business shall directly notify the consumer of
this new use and obtain explicit consent from the consumer to
use it for this new purpose.

(e) A business shall not collect categories of personal
information other than those disclosed in the notice at
collection. If the business intends to collect additional
categories of personal information, the business shall provide
a new notice at collection.

(f) If a business does not give the notice at collection to
the consumer at or before the collection of their personal
information, the business shall not collect personal
information from the consumer.

(g) Affiliates and third parties shall not sell consumer
personal information purchased from a business unless the
consumer has received notice and is provided an opportunity to
opt out of the resale of the consumer's personal information.

(h) Pricing incentives and prohibition of discrimination.
(1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights in this Act, including, but not limited to:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this Act.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing shall prohibit a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(3) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to
the consumer by the consumer's data.

(A) A business that offers any financial incentives regarding consumer personal information or deidentified information, shall notify consumers of the financial incentives in the consumer service agreement, website, online service or mobile application.

(B) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(C) A business shall not use financial incentive practices that are unjust, unreasonable, or coercive.

(i) A business that discloses personal information to a service provider shall not be liable under this Act if the service provider receiving the personal information uses it in violation of the restrictions set forth in the Act, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this Act for the obligations of a business for which it provides services as set forth in this Act.

(j) The obligations imposed on businesses by this Act do
not restrict a business' ability to:

(1) Comply with federal, state, or local laws, rules, regulations, or enforceable guidance.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Prevent, detect, or respond to identity theft, fraud, or other malicious or illegal activity.

(6) Collect, use, retain, sell, or disclose consumer's personal information that is deidentified or in the aggregate consumer information.

(k) Businesses, affiliates, and third parties shall take reasonable measures to protect customer's personal information from unauthorized use, disclosure, or access.

(1) In implementing security measures required by this subsection, a business, affiliate, and third party shall take into account each of the following factors:

(A) The nature and scope of the business;, affiliate's, or third party's activities;

(B) The sensitivity of the data processed;

(C) The size of the business, affiliate, or third
(D) The technical feasibility of the security measures.

(2) A business, affiliate, or third party may employ any lawful measure that allows the business, affiliate, or third party to comply with the requirements of this subsection.

(1) Risk assessments.

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

(2) Risk assessments conducted under subsection (a) must identify and weigh the benefits that may flow directly and indirectly from the processing to the business, consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can
be employed by the business to reduce such risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the business, affiliate, or third party and the consumer whose personal data will be processed, must factor into this assessment by the business, affiliate, or third party.

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

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

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

Section 40. Enforcement.

(a) Private right of action.

(1) Any consumer whose unencrypted or unredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than $100 and not greater than $750 per customer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.
(3) Nothing in this Act shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or Illinois Constitution.

(b) Attorney General enforcement. A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. The Attorney General has authority to enforce this Act as a violation of the Consumer Fraud and Deceptive Business Practices Act, subject to the remedies available to the Attorney General under the Consumer Fraud and Deceptive Business Practices Act.

Section 45. Applicability.

(a) This Act does not apply to personal information collected, processed, sold, or disclosed under:


   (3) The Fair Credit Reporting Act, and the rules promulgated under that Act.

(b) Nothing in this Act restricts a business' ability to collect or disclose a consumer's personal information if a consumer's conduct takes place wholly outside of Illinois. For
purposes of this Act, conduct takes place wholly outside of Illinois if the business collected that information while the consumer was outside of Illinois, no part of the sale of the consumer's personal information occurred in Illinois, and no personal information collected while the consumer was in Illinois is disclosed.

Section 50. Waivers; contracts. Any waiver of the provisions of this Act is void and unenforceable.

Section 55. Home rule preemption. Except as otherwise provided in this Act, the regulation of the activities described in this Act are the exclusive powers and functions of the State. Except as otherwise provided in this Act, a unit of local government, including a home rule unit, may not regulate the activities described in this Act. This Section is a denial and limitation of home rule powers and functions under subsection (h) of Section 6 of Article VII of the Illinois Constitution.

Section 97. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

Section 99. Effective date. This Act takes effect July 1, 2021.