INTERNATIONAL LAWYERS NETWORK

# 2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

# Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

# About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

## Authors of this guide:

### 1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

### 2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

# USA – Illinois

McDonald Hopkins' national data privacy and cybersecurity attorneys have a wealth of experience advising clients in a myriad of industries on the rapidly changing state, federal, international, and industry privacy and breach notification laws. McDonald Hopkins provides support on a daily basis and during investigations by state and federal regulators, as well assistance with:

- Breach coaching and incident notification
- International privacy compliance
- Payment cards and ecommerce
- Privacy litigation and class action
- Proactive measures and breach compliance
- Regulatory investigation and government response
- Vendor relationships

## Introduction

Illinois has enacted laws addressing rights and obligations related to data privacy. Companies and organizations that handle, collect, disseminate, or otherwise deal in nonpublic information have a number of requirements to bolster the data privacy rights and protections of residents. This paper will address the Illinois Personal Information Protection Act (815 ILCS 530/) as well as the proposed Illinois Data Protection and Privacy Act (HB3385).

## Governing Data Protection Legislation

**Overview of principal legislation – Personal Information Protection Act**

The principal data protection legislation in Illinois is the Personal Information Protection Act (815 ILCS 530/) ("PIPA"). PIPA was signed into law in 2005 and took effect in January 2006. The law was later updated to consider changes in technology and data collection methodology.

PIPA applies only to computerized data. Under PIPA, any data collector that maintains or stores, but does not own or license, computerized data that includes personal information as described further below, shall notify the owner or licensee of such information in the event of a breach of a security of the

## Contact Us

+1 (312) 280-0111
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
300 N. LaSalle Street, Suite 1400
Chicago, Illinois 60654 USA

data, if the personal information was or reasonably believed to have been acquired by an unauthorized person. This applies regardless of whether the data collector conducts business in Illinois. If notice is issued to more than 500 Illinois residents as a result of a single breach, the data collector must also notify the Attorney General of the breach. PIPA also requires data collectors to maintain reasonable security measures to protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure.

**Additional or ancillary regulation, directives or norms**

*Illinois Biometric Privacy Act*

The Illinois Biometric Privacy Act 2008 ("BIPA") (740 ILCS 14/1 to 740 ILCS 14/99) is significant as it was the first state legislation to address the collection and sharing of biometric information. The Act was passed in 2008, and other states began introducing legislation aimed at addressing biometric data thereafter. An overarching theme of BIPA is that an entity must maintain a reasonable standard of care in managing biometric information.

BIPA provides a set of rules for businesses to follow when collecting biometric data of state residents:

- Prior consent is required before the collection or disclosure of biometric data, such as fingerprints, voiceprints, or scans of hand or face geometry;
- Biometric data must be destroyed in a timely manner; and
- Biometric data must be securely stored.

*Student Online Personal Protection Act*

The Student Online Personal Protection Act ("SOPPA") (105 ILCS 85/1 to 105 ILCS 85/99) is the student data privacy law that regulates students' covered information by schools, education technology vendors, and the Illinois State Board of Education. It was signed into law in 2019 and outlines specific rights and responsibilities as it relates to covered information.

SOPPA requires that a school must provide notice to the parents of students within 30 days after determining that a breach of covered information occurred. It further requires that schools must implement and maintain reasonable security procedures to protect covered information from unauthorized access, destruction, use, modification, or disclosure. Additionally, SOPPA outlines requirements as to the deletion of covered information.

**Upcoming or proposed legislation**

*Illinois Data Protection and Privacy Act*

*The Illinois Data Protection and*

Privacy Act (HB3385) was introduced by Rep. Abdelnasser Rashid in the 2023 House session. If passed, the bill would implement data minimization practices. Additionally, the bill outlines data subjects' rights, including the right to access, rectification, deletion, data portability, and object to data processing. The bill also includes protections for minors, including a prohibition against engaging in targeted advertising if the covered entity is aware that the individual is a minor, or transferring the data of a minor to a third party without express consent from a parent or guardian. The bill further addresses the establishment of more practical data security practices, such as employee trainings.

If passed, the bill would provide significant protections to Illinois residents.

## Legislative Scope of the Illinois Personal Information Protection Act (815 ILCS 530/)

The Illinois general data breach notification statute, PIPA, applies to any data collector that owns or licenses computerized personal information concerning an Illinois resident ("covered entity"). A data collector is any entity that handles, collects, disseminates, or otherwise deals with nonpublic personal information for any purpose, including but not limited to corporations, government agencies, universities, financial institutions, and retail operators.

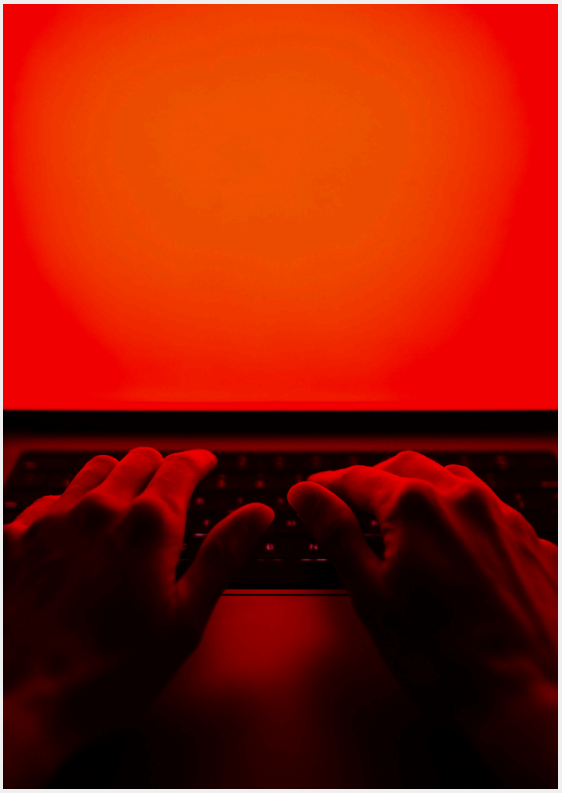
**Definition of personal information**

Under PIPA, "personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements when not encrypted or redacted:

- Social Security number.
- Driver's license number or State identification card number.
- Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Medical information.
- Health insurance information.
- Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Personal information also includes a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Of note, personal information does not include publicly available information that is lawfully made available to the general public from government records.



**Definition of different categories of personal data**

PIPA further defines "health insurance information" to include: an individual's health insurance policy number, subscriber identification number, unique identifier used to identify an individual, medical information in a health insurance application, and claims history.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or treatment or diagnosis by a healthcare professional.

**Statutory exemptions**

Entities subject to the privacy and security standards outlined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Health Information Technology for Economic and Clinical Health Act ("HITECH") will be in compliance with PIPA's breach notification requirements if they provide a copy of any breach notice sent to Health and Human Services to the Illinois Attorney General within five days.

**Territorial and extra-territorial application**

PIPA, applies to any data collector that owns or licenses computerized personal information concerning an Illinois resident, regardless of the location of the data collector.

## Legislative Framework

**Key Stakeholders**

*Data Collector*

"Data Collector" refers to, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any reason, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

A data collector that owns or licenses personal information concerning an Illinois resident is responsible for securely maintaining that information, and notify the resident in the event of a breach of the security of the system data following discovery of the breach. The notification must be made expediently and without unreasonable delay.

Notice to individuals may be provided in one of the following ways:

- Written notice;
- Electronic notice, if it is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
- Substitute notice, if the data collector can demonstrate that the cost of providing notice would exceed $250,000 or if the notice population exceeds 500,000. Substitute notice can also be provided in the event the data collector does not have sufficient contact information. Substitute notice can include:
    - o Email notice;
    - o Conspicuous notice posted on the data collector's web page; or
    - o Notification to major state wide media, or local media if the breach impacts residents in one geographic area.

Notification to more than 500 Illinois residents as a result of a single breach requires the covered entity provide notice to the Attorney General. Such notification must include a description of the breach, the number of Illinois residents impacted, and steps the data collector has taken in relation to the incident. The Attorney General may make this information public.

*State Agency*

PIPA contemplates the roles and responsibilities of state agencies. Under the statute, any State agency that collects personal information concerning an Illinois resident is required to provide notice in the event of a breach of the security of the system data or written material following discovery of the breach. The notification must be made expediently and without unreasonable delay.

Any State agency that notifies more than 1,000 individuals in connection with a single breach is required to notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p). Further, any State agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents must provide notice to the Attorney General with the information described above.

**Regulatory Authorities and consequences of non-compliance**

The provisions set forth in 815 ILCS §§

530/1 through 530/25 are enforced by the Illinois Attorney General. Violations of the statute are considered unlawful practices under the Consumer Fraud and Deceptive Business Practices Act and as such are subject to all applicable penalties under the Act. To that end, covered entities that fail to comply with the statutory requirements are subject to both monetary and civil liability penalties. This includes:

- Injunction;
- The inability to conduct business within Illinois;
- Civil penalties up to $50,000;
- Additional penalties of $50,000 per violation;
- Additional penalties of $10,000 per violation for acts committed against a person 65 years or older.

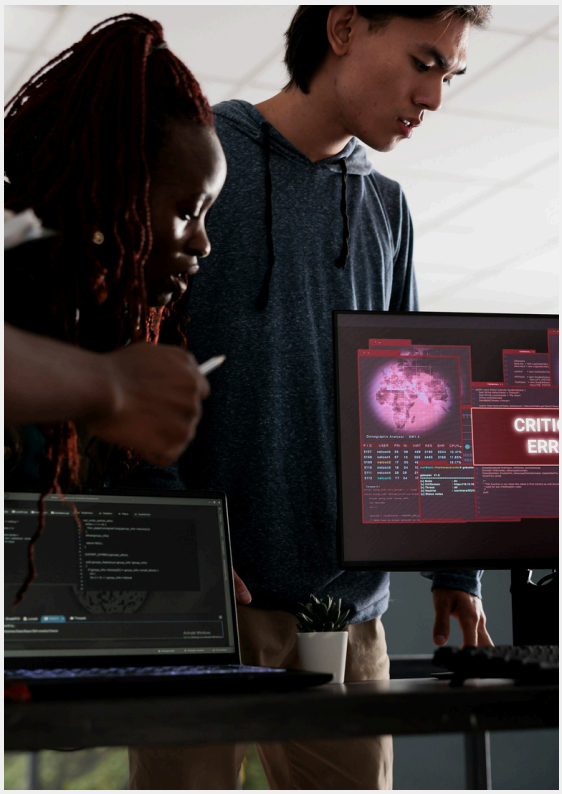
## Legislative Scope of the proposed Illinois Data Protection and Privacy Act (HB3385)

The proposed Data Protection and Privacy Act ("DPPA") applies to any entity that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data ("covered entity"). A covered entity does not include a federal, State, tribal, territorial, or local government entity, or an entity acting as a service provider to the aforementioned government entity. The definition also does not include nonprofits, national resource centers, or clearinghouses providing assistance to various vulnerable groups as defined further in the bill.

The DPPA provides that a covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate.

**Definition of covered data**

Under the DPPA, "covered data" refers to information, including derived data and unique identifiers that identifies or is linked to, alone in combination with other information, to an individual or a device that identifies or is linked to an individual. Covered data does not include de-identified data, employee data, or publicly available information.



https://www.mcdonaldhopkins.com/

**Other key definitions**

A "data broker" is a covered entity whose principal source of revenue is derived from processing or transferring covered data that the entity did not collect directly from the associated individuals. This does not include employee data collected by and received from a third party for the sole purpose of providing benefits to the employee.

The bill defines "biometric information" as covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that can be linked to the individual. This can include fingerprints, voice prints, retina scans, or hand mapping.

"Collection" refers to the buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.

"Control" means an entity that has ownership of another entity, control over a voting majority, or the power to exercise controlling influence over the management of an entity.

A "covered minor" refers to an individual under the age of 17.

To "process" covered data refers to conducting or directing any operation on covered data, including analyzing, organizing, retaining, storing, using, or otherwise handling said data.

"Sensitive covered data" refers to the following:

- A government-issued identifier, such as a Social Security number, passport number, or driver's license number;
- Any information that describes or reveals the health condition or diagnosis of an individual;
- Financial account number or credit or debit card number;
- Biometric information;
- Genetic information;
- Precise geolocation information;
- Private communications such as text messages;
- Account or device log-in credentials;
- Information identifying sexual behaviour;
- Calendar information, address book information, audio recordings, or videos maintained for private use, regardless of what information is contained therein;
- Photos or videos showing nudity or partial nudity of an individual;
- Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service;
- Information about an individual when the covered entity or service provider knows the individual is a covered minor;
- Race, color, ethnicity, religion, or union membership;
- Information identifying an individual's online activity over time and across websites;

- Any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data described above.

**Extra-territorial application**

If passed, the DPPA would apply to covered entities that collect, process, or transfer covered data of Illinois residents, regardless of the location of the entity.

## Legislative Framework

**Requirements for Data Collection, Processing, or Transfer**

Should the DPPA pass, it would only allow for the collection, processing, or transfer of covered data to the extent it is reasonably necessary and proportionate to provide a specific product or service requested by the individual. The bill describes specific scenarios in which data collection, processing, or transfer would be legitimate.

The DPPA also prohibits a covered entity from transferring covered data without obtaining an individual's affirmative express consent. Moreover, an individual must have the means to withdraw any affirmative express consent previously provided with respect to the processing or transfer of covered data. Notwithstanding this, a covered entity that directly engages in collection, processing, or transfer activities enumerated in the bill need not allow opt-out mechanisms.

Under the bill, a covered entity may not collect, process, or transfer data in a discriminatory manner.

**Data storage and retention timelines**

Covered data must be disposed when it is no longer necessary for the purpose for which it was collected, processed, or transferred, unless an individual has provided affirmative express consent to retention. Such disposal includes permanently destroying or otherwise modifying the data to make it permanently indecipherable.

**Data protection and security practices and procedures**

The DPPA would require a covered entity to establish, implement, and maintain reasonable data security practices to protect the covered data against unauthorized access or acquisition. If passed, practices should include:

- Identifying and assessing material risks and vulnerabilities in security systems;
- Taking preventative corrective actions to mitigate foreseeable risks;
- Disposing of covered data when it is no longer necessary for the purpose for which it was collected, processed, or transferred, unless affirmative express consent was obtained for additional retention;
- Providing employee training to safeguard covered data;

- Designating an officer to maintain and implement practices;
- Implementing procedures to detect, respond to, and recover from security incidents.

## Minors' Data

- A covered entity would not be permitted to engage in targeted advertising to known minors. Moreover, under the bill, a covered entity may not transfer covered data of a covered minor to a third party without affirmative express consent of the minor's guardian, with some exceptions.

## Regulatory Authorities

If passed, the DPPA would enable the Attorney General to adopt rules for purposes of carrying out the Act. This would include adjusting definitions, updating or adding categories to definitions, establishing rules and procedures to facilitate an individual's ability to delete or correct covered data, and establishing additional exceptions to protect the rights of individuals.

Additionally, any person subject to a violation of the DPPA could bring a civil action against the violating entity. If the plaintiff prevails, the court may award the plaintiff compensatory, liquidated or punitive damages. In addition, a court could award injunctive relief, declaratory relief, and/or attorney's fees.

**Consequences of non-compliance**

The Attorney General, State's Attorney, or municipality's attorney may bring a civil action against any covered entity that violates the DPPA. Penalties include:

- Enjoining violating acts;
- Enforcing compliance with the DPPA;
- Obtaining damages, civil penalties, restitution, or other compensation on behalf of residents of Illinois;
- Obtaining reasonable attorneys' fees or other litigation costs.

## Conclusion

The Illinois legislative landscape includes robust requirements for data collectors in the event of a data breach. The Illinois Data Protection and Privacy Act includes specific parameters surrounding the protection and breach of resident data. The proposed Data Protection and Privacy Act would add to the privacy landscape in Illinois by providing individuals with increased rights as it relates to their personal data, as well as imposing increased responsibilities on entities that collect, process, and transfer such data.

## Contact Us

+1 (312) 280-0111
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
300 N. LaSalle Street, Suite 1400
Chicago, Illinois 60654 USA