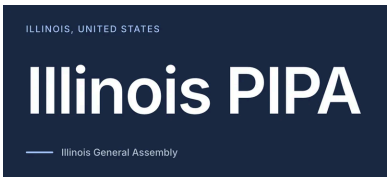
SmartSuite

Framework / Privacy / Global Privacy Regulations

Illinois Personal Information Protection Act (815 ILCS 530)

Illinois PIPA (815 ILCS 530) requires data collectors to protect Illinois residents' personal information, notify residents of a breach and notify the Attorney General above 500 residents.



What it is

The Illinois Personal Information Protection Act (815 ILCS 530) is the Illinois General Assembly's data security and breach notification law. It requires any “data collector” that handles personal information of Illinois residents to maintain reasonable security measures (Section 45), to notify residents of a breach of the security of the system data (Section 10) and, above 500 residents, to notify the Attorney General. It took effect on January 1, 2006 (Public Act 94-36), and the current text carries amendments through Public Act 101-343, effective January 1, 2020.

A data collector includes government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators and any other entity that handles, collects or disseminates nonpublic personal information (Section 5). Personal information means a name combined with a Social Security number, driver's license or State identification number, financial account or card number, medical information, health insurance information or unique biometric data, or a user name or email address combined with a password or security question and answer.

At a glance

PUBLISHER Illinois General Assembly	TYPE Regulation	VERSION 815 ILCS 530, Public Act 94-36 as amended through Public Act 101-343
EFFECTIVE January 1, 2006 (latest amendment, Public Act 101-343, effective January 1, 2020)	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION Illinois	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Medium

Source: ilga.gov/Legislation/ILCS/Articles?ActID=2702&ChapterID=67

Why it matters

- **A defined set of data elements** Section 5 lists the combinations that count as personal information, including medical information, health insurance information and unique biometric data, so scope can be inventoried field by field.
- **Encryption changes the outcome** Name or data elements that are encrypted or redacted fall outside the definition unless the keys to read them were acquired through the breach (Section 5).
- **Security reaches vendors** A contract for the disclosure of personal information must require the recipient to implement and maintain reasonable security measures (Section 45(b)).
- **Defined paths to deemed compliance** Compliance with the GLBA Section 501(b) standards, with HIPAA and HITECH (Section 50), with a stricter law (Section 45(c)) or with your own notification procedures (Section 10(d)) is deemed compliance under the sections stated.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports IL PIPA (815 ILCS 530)

Personal Information Inventory

Record where each Section 5 data element is stored, whether it is encrypted or redacted and who holds the keys.

Reasonable Security Measures Register

Map safeguards to Section 45(a), with owners, test results and the evidence behind each control.

Vendor Contract Security Terms

Track every contract that discloses personal information and confirm the Section 45(b) security clause and the Section 10(b) duty to notify the owner.

Breach Assessment and Resident Notice

Log the discovery date, the data involved, any law enforcement delay, the notice method and the Section 10(a) content for each affected resident.

Attorney General Notice Tracker

Count affected Illinois residents against the 500 threshold, record the Section 10(e) report and, for HIPAA entities, the Section 50 five-business-day notice.

Disposal Records

Log how paper and electronic media were destroyed and how third-party disposal vendors are monitored (Section 40).

Common framework mappings

CCPA/CPRA | CIS Controls v8.1 | GDPR | GLBA Safeguards Rule (16 CFR Part 314) | HIPAA (NIST SP 800-66 Rev. 2) | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1

Official resources

Personal Information Protection Act (P.A. 99-0503; 815 ILCS 530)

Defines obligations of data collectors and State agencies regarding notification of breaches and security requirements.

ilga.gov/legislation/publicacts/view/099-0503

Personal Information Protection Act (815 ILCS 530/10-12) – Notice of Breach; State Agency Requirements

Outlines breach notification timelines and required content for State agencies and when to notify the Attorney General.

ilga.gov/Legislation/ILCS/Articles?ActID=2702&ChapterID=67

SB1624 Amendment to PIPA (815 ILCS 530/10, 55)

Amends breach notification thresholds and requires annual Attorney General reporting to the General Assembly.

ilga.gov/legislation/BillStatus.asp?DocTypeID=SB&DocNum=1624&GAID=16&SessionID=110&LegID=139584

Frequently asked questions

Who must comply with the Illinois Personal Information Protection Act?

Any “data collector” that handles, collects or disseminates nonpublic personal information, including government agencies, universities, corporations, financial institutions and retailers (Section 5). It protects the personal information of Illinois residents. Covered entities and business associates that comply with HIPAA and HITECH are deemed compliant under Section 50, and entities that meet the GLBA Section 501(b) standards are deemed compliant with Section 45.

How quickly must Illinois residents be notified of a breach?

Notice must be given in the most expedient time possible and without unreasonable delay, after allowing for the steps needed to determine the scope of the breach and restore the system (Section 10(a)). The Act sets no fixed number of days for private data collectors. A written law enforcement request can delay notice until it no longer interferes with the investigation (Section 10(b-5)).

 © 2026 SmartSuite Inc. All rights reserved.

When must the Illinois Attorney General be notified?

A data collector that notifies more than 500 Illinois residents about a single breach must also notify the Attorney General, no later than the consumer notice, describing the breach, the number of residents affected and the steps taken (Section 10(e)). State agencies report above 250 residents within 45 days (Section 12(e)). A HIPAA covered entity or business associate that notifies the Secretary of Health and Human Services notifies the Attorney General within five business days (Section 50).

Does encrypting data avoid the notification duty?

Only in part. Personal information is defined as a name or other listed data elements that are unencrypted or unredacted, or encrypted or redacted but with the keys acquired without authorization through the breach (Section 5). Encrypted data whose keys were not taken falls outside the definition. Online account credentials follow the same rule under paragraph (2) of the definition.

What are the penalties under the Act?

A violation is an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act (Section 20). For improper disposal, the Attorney General can impose a civil penalty of up to $100 per individual, capped at $50,000 per instance, and can seek other relief in circuit court (Section 40(d) and (e)). Waivers of the Act are void (Section 15).

License included / downloadable: Yes The Act is Illinois law. Its text is free to read on the Illinois General Assembly website (ilga.gov).

Full framework page and mappings: smartsuite.com/frameworks/illinois-personal-information-protection-act-815-ilcs-530

© 2026 SmartSuite Inc. All rights reserved.