Illinois Biometric Information Privacy Act (740 ILCS 14)

BIPA

Illinois BIPA regulates how organizations collect, store, and disclose biometric identifiers, requiring notice, consent, retention limits, and security.

What it is

The U.S. Illinois Biometric Information Privacy Act (BIPA) is a state data protection law that governs the collection, storage, and use of biometric identifiers and biometric information. BIPA establishes strict requirements for organizations to safeguard sensitive biometric data, such as fingerprints, facial recognition data, and iris scans, to protect individual privacy rights.

Enacted by the Illinois General Assembly in 2008, BIPA applies to private entities operating within Illinois that collect or handle biometric information from residents. The law mandates informed consent, secure data storage, and limitations on disclosure, making it central to privacy compliance programs for organizations leveraging biometric technologies for authentication, identity management, or employee tracking.

At a glance

PUBLISHER Illinois General Assembly	TYPE Regulation	VERSION 2008
EFFECTIVE October 3, 2008	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION Illinois	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

Source: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Why it matters

- **Strengthen data protection practices** Enhance safeguards for sensitive biometric identifiers, reducing the likelihood of unauthorized access and potential misuse of personal information.
- **Improve regulatory compliance** Support adherence to state privacy laws, helping organizations prevent costly legal actions and maintain compliance with Illinois requirements.
- **Increase audit readiness** Enable organizations to demonstrate clear, documented policies and practices for collecting and handling biometric data during compliance reviews.
- **Enhance individual privacy** Build trust with users and employees by ensuring transparent notice, obtaining informed consent, and prioritizing personal privacy interests.

 Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports BIPA (740 ILCS 14)

Biometric Data Governance Requirements

Structure requirements for collection, use, storage, and destruction of biometric identifiers and information.

Biometric Data Inventory and Classification

Track systems, datasets, and processes that collect or store biometric data.

Consent and Disclosure Management

Manage written consent, disclosures, and authorization records required before collecting biometric data.

Retention and Destruction Policy Tracking

Track retention schedules and ensure timely deletion of biometric data in accordance with legal requirements.

Access Control and Data Protection Measures

Manage access permissions, encryption, and safeguards protecting biometric information from unauthorized access.

Biometric Data Protection Compliance Reporting

Provide dashboards showing consent status, retention compliance, and overall biometric data protection posture.

Common framework mappings

SOC 2 | CCPA/CPRA | GDPR | HIPAA | ISO 27701 | NIST Privacy Framework v1.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1

Official resources

Illinois Biometric Information Privacy Act Text

Official legal text outlining the requirements and obligations under BIPA.

ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0994

Frequently asked questions

What is the Illinois Biometric Information Privacy Act (BIPA) used for?

BIPA is designed to regulate the collection, use, storage, and destruction of biometric identifiers and information such as fingerprints, facial recognition data, and iris scans. Its primary purpose is to protect the privacy and security of individuals' biometric data and prevent its unauthorized use or disclosure.

Is compliance with BIPA mandatory?

Yes, BIPA is a mandatory state law for any private entity operating in Illinois that collects, stores, or processes biometric data from individuals. Non-compliance can result in significant statutory damages and legal action, including private rights of action.

Who does BIPA apply to?

BIPA applies to any private entity that collects, captures, purchases, receives through trade, stores, or otherwise obtains biometric identifiers or biometric information of individuals located in Illinois. The law excludes government agencies, law enforcement, courts, and financial institutions governed by other federal laws.

What are the key compliance requirements of BIPA?

Organizations must obtain informed, written consent before collecting or disclosing biometric information. They are also required to develop a publicly available written policy outlining their retention schedule and guidelines for permanent destruction of biometric data, and must safeguard such data using reasonable standards of care.

How do organizations implement BIPA requirements?

Implementation involves establishing procedures for obtaining explicit written consent, developing and publishing a biometric data retention and destruction policy, and deploying appropriate technical and administrative safeguards for data protection. Regular training and updates can help ensure consistent BIPA compliance across the organization.

© 2026 SmartSuite. All rights reserved.

How does BIPA compare to other privacy laws like the GDPR or CCPA?

While BIPA focuses specifically on biometric data, the GDPR (EU) and CCPA (California) address a broader range of personal data types. BIPA is notable for its strict consent requirements and private right of action, making its enforcement and litigation risk higher than some comparable state or federal privacy laws.

What are the ongoing compliance obligations under BIPA?

Ongoing obligations include maintaining up-to-date privacy policies, regularly reviewing data retention practices, ensuring all appropriate consent documents are collected and stored, and continuously monitoring for new technologies or uses of biometric data that may introduce new compliance risks.

How would SmartSuite support Illinois Biometric Information Privacy Act (BIPA)?

SmartSuite can help organizations manage BIPA compliance by tracking biometric data risks, documenting and managing control activities, collecting evidence of consent and data handling policies, supporting audit readiness through automated workflows, and generating compliance reports to demonstrate adherence to BIPA requirements.

License included / downloadable: Yes The Illinois Biometric Information Privacy Act is published by the Illinois General Assembly and is publicly available on the ILGA website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-illinois-biometric-information-privacy-act-bipa