

Illinois Identity Protection Act (815 ILCS 530)

Illinois' Identity Protection Act requires organizations to safeguard personal information and notify individuals of security breaches.



What it is

The U.S. Illinois Identity Protection Act (IPA) is a state-level privacy regulation that helps organizations safeguard the confidentiality of an individual's Social Security Number (SSN) and other sensitive personal identifiers. Its primary purpose is to prevent the unauthorized disclosure and misuse of personal information, thereby enhancing data protection and supporting privacy risk management for entities handling such data.

Enacted by the State of Illinois and enforced by state governmental authorities, the IPA applies to both public and private sector organizations operating in Illinois that collect, use, or disclose SSNs during business or administrative activities. The Act outlines specific requirements related to the collection, storage, handling, and disposal of SSNs, and sets standards for privacy governance to minimize the risk of identity theft.

At a glance

PUBLISHER	TYPE	VERSION
Illinois General Assembly	Regulation	2010 (P.A. 96-874, eff. 6-1-10) ([law.justia.com](https://law.justia.com/codes/illinois/chapter-5/act-96-874) (addition of section 20) ([ilga.gov](https://www.ilga.gov/reports/ReportsSubmitted/3074RSGAEmail5904RSGAAttachSSN%20Protection%20Act%20ActID=2368) (utm_source=openai)))
EFFECTIVE	DOMAIN	FAMILY
June 1, 2010	Privacy	Global Privacy Regulations
REGION	ADOPTION MODEL	IMPLEMENTATION COMPLEXITY
Illinois	Regulatory Compliance	Moderate

Source: <https://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=005000170HArt%2E+3&ChapterID=1&ActID=2368>

Why it matters

- **Strengthen data handling practices** Promote responsible collection, use, and protection of personal information such as social security numbers to reduce misuse and accidental exposure.
- **Enhance regulatory alignment** Ensure organizational policies align with state legal requirements, supporting consistent privacy and compliance standards across business processes.
- **Improve audit readiness** Facilitate thorough documentation of data protection procedures, making compliance verification and audit processes more efficient and less resource-intensive.
- **Reduce reputational risk** Minimize the likelihood of public exposure or legal action resulting from improper handling or disclosure of protected identity information.

How SmartSuite supports 815 ILCS 530

Personal Data Safeguards Library

Structure safeguards for protecting personal data, including access control, encryption, and secure storage practices.

Data Inventory and Classification

Track personal information types, storage locations, and processing systems subject to IPA requirements.

Identity Protection Policies and Accountability

Manage identity protection policies, procedures, and accountability across business functions.

Access and Personal Information Management

Manage user permissions, authentication controls, and proper handling of sensitive personal information.

Security Incident and Notification Management

Track security incidents and manage notification obligations for affected individuals and regulators.

Identity Protection Compliance Reporting

Provide dashboards showing data protection posture, breach readiness, and compliance with Illinois identity protection requirements.

Common framework mappings

CIS Controls v8.1

COBIT 2019

FERPA

GDPR

GLBA Safeguards Rule (16 CFR Part 314)

HIPAA

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

Official resources

Illinois Identity Protection Act (5 ILCS 179) — Full statutory text of the Identity Protection Act as enacted by the Illinois General Assembly.

ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3573&ChapterID=58

Illinois Attorney General – SSN Protection Task Force Report (2025) — Describes updates and policies replacing SSNs, including section 20 added in 2021.

illinoisattorneygeneral.gov/Page-Attachments/IllinoisSocialSecurityNumberTaskForceReport2025.pdf

Department of Children and Family Services Administrative Procedure #27 – Identity Protection — Provides agency-specific policy procedures for complying with the Identity Protection Act.

dcfs.illinois.gov/content/dam/soi/en/web/dcfs/documents/about-us/policy-rules-and-forms/documents/administrative-procedure/administrative-procedure-27.pdf

Illinois Department of Corrections Administrative Directive 01.02.108 – Identity Protection — Details internal DOC directives on safeguarding SSNs under the Identity Protection Act.

idoc.illinois.gov/content/dam/soi/en/web/idoc/aboutus/policies/policies/administration-organization-and-management/102108%20Identity%20Protection.pdf

Frequently asked questions

What is the Illinois Identity Protection Act (IPA) used for?

The Illinois Identity Protection Act (IPA) is designed to safeguard the handling, use, and disclosure of Social Security Numbers (SSNs) by government agencies and other entities collecting this sensitive information in Illinois. Its goal is to prevent identity theft and unauthorized access to personally identifiable information.

Is compliance with the Illinois IPA mandatory?

Yes, compliance with the Illinois IPA is mandatory for state and local government agencies, as well as any contractors or third parties acting on their behalf that collect or process SSNs. Noncompliance can result in administrative penalties and legal liabilities.

Who does the Illinois IPA apply to?

The IPA applies primarily to Illinois state and local government agencies, their employees, and vendors who collect, maintain, or use SSNs. It also extends to any organization or party performing contracted work for these entities involving SSN data.

What are the key requirements and concepts of the Illinois IPA?

Key requirements of the Illinois IPA include adopting a written identity protection policy, restricting public display or transmission of SSNs, and training staff on proper handling and safeguarding practices for SSN data. Organizations must limit access to SSNs to only those who need it for official purposes.

How should organizations implement Illinois IPA requirements?

Organizations should begin by conducting a data inventory to identify where SSNs are collected and stored, establish a written protection policy, and ensure technical and administrative controls are in place. Regular staff training and process reviews are essential for effective implementation.

How does the Illinois IPA relate to other privacy laws or frameworks?

The Illinois IPA aligns with broader privacy regulations like HIPAA and the Gramm-Leach-Bliley Act by emphasizing the protection of personally identifiable information. However, it focuses specifically on SSNs and applies to government agencies within Illinois, complementing but not replacing federal requirements.

What are the ongoing compliance obligations under the Illinois IPA?

Ongoing obligations include annual policy reviews and updates, continual employee training, monitoring access and use of SSNs, and timely remediation of violations. Agencies must also respond appropriately to SSN-related incidents and update procedures as laws evolve.

How would SmartSuite support Illinois Identity Protection Act (IPA) compliance?

SmartSuite can support Illinois IPA compliance by centralizing risk tracking for SSN-related exposures, managing policies and controls, and organizing evidence such as employee training and policy acknowledgments. The platform can streamline audit preparations, provide reporting on compliance status, and monitor for changes or incidents, supporting agencies in maintaining and demonstrating IPA adherence.

License included / downloadable: Yes The Illinois Identity Protection Act is published by the Illinois General Assembly and is publicly available through official state legislative publications. License included with platform

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