



Indiana Consumer Data Protection Act ("INCDPA") Compliance Snapshot

Understand the Law. Identify Your Obligations. Prepare for Compliance.

This CLIClaw Compliance Snapshot provides a concise overview of the Indiana Consumer Data Protection Act ("INCDPA"), including its applicability, consumer privacy rights, key business obligations, third-party requirements, enforcement provisions, and compliance considerations.

Designed as a practical reference for businesses, the snapshot helps organizations understand the law's principal requirements, evaluate potential applicability, and identify areas that may require additional compliance planning or operational review.

Use this snapshot as a starting point for understanding Indiana's privacy requirements and determining whether further assessment, implementation, or legal guidance is needed.

DISCLAIMER

These materials are provided for informational and compliance support purposes only and are not intended as legal advice. Use of these materials does not establish an attorney-client relationship.

Organizations are responsible for evaluating applicable legal requirements and should consult qualified legal counsel regarding specific obligations.

CLIClaw makes no warranties regarding the completeness or applicability of these materials and disclaims liability for reliance on their use.

INDIANA CONSUMER DATA PROTECTION ACT (INCDPA)

2026 COMPLIANCE SNAPSHOT



Effective January 1, 2026.

Indiana law establishes consumer privacy rights and obligations for covered controllers that collect, use, or disclose personal data of Indiana residents.

01

APPLICABILITY

Which Organizations May Be Covered?



Control or process personal data of **100,000 or more** Indiana consumers in a calendar year;
OR



Control or process personal data of **25,000 or more** Indiana consumers in a calendar year
AND derive more than 50% of gross revenue from the sale of personal data.



Nonprofit organizations and certain other entities are exempt.

02

INDIANA RESIDENT RIGHTS

What Rights Do Consumers Have?



Confirm

Consumers can confirm whether an organization is processing their personal data.



Access

Consumers can access their personal data.



Correct

Consumers can correct inaccuracies in their personal data.



Delete

Consumers can delete their personal data, subject to certain exceptions.



Data Portability

Consumers can obtain a copy of their personal data in a portable format.



Opt-Out Rights

Consumers can opt out of:

- Targeted advertising;
- The sale of personal data; and
- Certain profiling for decisions that produce legal or similarly significant effects.

03

KEY CONTROLLER OBLIGATIONS

What Must Covered Organizations Do?



Privacy Notice

Provide a clear and accessible privacy notice that meets INCDPA requirements.



Consumer Rights Process

Establish and maintain a process to receive, verify, and respond to consumer requests, including an appeals process.



Data Minimization

Collect, use, and retain only personal data that is adequate, relevant, and reasonably necessary for the disclosed purposes.



Security Safeguards

Implement and maintain reasonable administrative, technical, and physical safeguards to protect personal data.



Sensitive Data Consent

Obtain consumer consent before processing sensitive data, subject to statutory provisions.



Data Protection Impact Assessments

Conduct and document assessments for processing that presents a heightened risk of harm to consumers, as required by law.

04

SENSITIVE DATA

What Additional Requirements Apply?



Definition

Sensitive data includes precise geolocation information, identifying biometric data, genetic data, certain health information, and children's data.



Consent Requirement

Obtain consumer consent before processing sensitive data, subject to statutory provisions and exceptions.



Children's Data

Additional protections apply to the personal data of known children.



Precise Geolocation

Processing precise geolocation information is subject to enhanced requirements.



Additional Restrictions

The law imposes specific requirements and limitations on the processing and sale of sensitive data.

05

SERVICE PROVIDERS, CONTRACTORS & SALES

What Requirements Apply to Third Parties?



Service Providers and Contractors

Use written controller-processor contracts that include required terms, including obligations to protect personal data, assist with consumer requests, and maintain confidentiality.



Sale of Personal Data

"Sale" means an exchange of personal data for money, subject to statutory exclusions.



Disclosures and Opt-Outs

Disclose sales of personal data and the use of personal data for targeted advertising and provide an easy way for consumers to opt out.

06

DATA RETENTION & GOVERNANCE

How Should Personal Data Be Managed?



Retention Limits

Retain personal data only for as long as is adequate, relevant, and reasonably necessary for the purposes disclosed in the privacy notice.



Data Governance

Maintain reasonable policies, procedures, and oversight to ensure compliance with the INCDPA.



Ongoing Compliance

Regularly evaluate and update data practices to reflect legal requirements and applicable risk assessments.



ENFORCEMENT

- Enforced by the Indiana Attorney General.
- No private right of action.
- Civil penalties of up to \$7,500 per violation, subject to statutory enforcement procedures.



CLIClaw
Center for Legal Internet Compliance

General information only; not legal advice.
Last reviewed: October 16, 2026

© 2026 CLIClaw
www.cliclaw.com

