Akin®

Indiana Data Protection Act: What Businesses Need to Know

August 21, 2023

Reading Time : **10 min**

By: Natasha G. Kohne, Joseph Hold

The recent enactment of the Indiana Consumer Data Protection Act (INCDPA) has placed Indiana as the seventh comprehensive data privacy law. Indiana's law arrives on the heels of the Iowa Act Relating to Consumer Data Protection (ICDPA), which we have summarized here, and adopts a lengthy time period to come into compliance, taking effect on January 1, 2026.

The Indiana law is similar to the business-friendly Virginia Consumer Data Protection Act (VCDPA), Utah Consumer Privacy Act (UCPA) and ICDPA, as opposed to the more consumer-friendly Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA) and California Consumer Privacy Act (CCPA) (as amended by the California Privacy Rights Act (CPRA)).

Key Provisions

- *Right to Correct* – consumers have the right to correct inaccuracies only for data they previously provided to the controller.
- *Copy or Summary Discretion* – controller has discretion whether to send a copy of a consumer's personal data or a summary of that data in response to an access request.
- *Sale of Personal Information* – like the Virginia and Utah laws, the definition of "sale" of personal information only pertains to data exchanged for monetary consideration.
- *Opt-Out Rights* – much like the Virginia, Colorado and Connecticut laws, consumers have the right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data and the use of personal data for certain profiling activities.
- *Right to Cure* – the INCDPA provides a 30-day cure period for alleged violations.

- *Extended Effective Date* – the law does not take effect until almost three years from enactment, on January 1, 2026.

Who Must Comply with the INCDPA?

Similar to the other comprehensive state privacy laws, as well as Europe's General Data Protection Regulation (GDPR), the INCDPA applies to "controllers"—meaning a person that determines the purposes and means of processing personal data, and "processors"—meaning a person that processes that data on behalf of the controller. The INCDPA applies to a person conducting business in Indiana or providing products or services targeted to Indiana residents that either:

- Control or process personal data of at least 100,000 Indiana consumers.
- Control or process the personal data of at least 25,000 Indiana consumers while deriving over 50% of gross revenue from selling personal data.[1]

However, the INCDPA does not feature a minimum annual revenue threshold, so relatively small businesses could still find themselves subject to its provisions.

What Information Is Covered?

The INCDPA applies to "personal data," which it defines as "information that is linked or reasonably linkable to an identified or identifiable individual."[2]

The law also specifies that "sensitive data" includes genetic or biometric data, data of known children, precise geolocation data and personal information revealing racial or ethnic origin, religious beliefs and health status.[3]

What Are the Notable Exemptions?

As seen in other state privacy laws, the INCDPA includes entity- and data-level exemptions.

Data-Level Exemptions

The INCDPA excludes data that is de-identified, aggregated or publicly available.[4] Also, as in Virginia, Colorado, Connecticut, Utah and Iowa, the INCDPA expressly excludes from the definition of "consumer," individuals acting in "a commercial or employment context,"[5] which

means that data collected from individuals acting in these capacities is not protected under the law. Other data-based exemptions include data subject to the Graham-Leach-Bliley Act (GLBA), and the Family Education Rights and Privacy Act (FERPA),[6] as well as personal data processed in compliance with the Fair Credit Reporting Act (FCRA) and the Driver's Privacy Protection Act (DPPA).[7]

The INCDPA also includes several exemptions around health data, including an exemption for protected health information under the Health Insurance Portability and Accountability Act (HIPAA) and information and documents created for the Health Care Quality Improvement Act (HCQIA).[8] Patient safety work product created for the Patient Safety and Quality Improvement Act (PSQIA) is also exempt, along with information used only for public health activities and purposes as authorized by HIPAA. There are also a number of carve-outs specifically related to personal information collected, processed or sold in connection with certain types of research, such as human subject research and public or peer-reviewed scientific or statistical research in the public interest.[9]

Entity-Level Exemptions

The INCDPA contains a familiar list of entity-level exclusions, as it does not apply to nonprofits, institutions of higher education, public utilities, financial institutions and affiliates subject to the GLBA and entities subject to HIPAA.[10] The law also does not apply to government entities or third parties acting under contract on behalf of government entities.

The Indiana law also contains a unique exemption, specifically excluding licensed riverboats using facial recognition technology approved by the Indiana gaming commission from coverage.[11]

What Rights Do Indiana Consumers Have?

The INCDPA provides consumers with rights similar to those found in other comprehensive state privacy laws, but with some unique features. For instance, consumers have the rights to: (1) know whether a controller is processing the consumer's personal data and if so, to access that data; (2) request correction of inaccuracies, but only for data they provided to the controller (as opposed to data about them collected from other sources); (3) obtain a copy or representative summary of their data; (4) request deletion of that data; and (5) opt out of the

processing of personal data for targeted advertising, the sale of personal data and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[12] On the other hand, the INCDPA does differ slightly from other comprehensive privacy laws. For example, in responding to requests for access, the controller has the discretion to either send a copy of the personal data or a "representative summary" of that data.[13] Additionally, similar to the Utah, Virginia and Iowa laws, the INCDPA does not appear to explicitly require organizations to recognize universal opt-out mechanisms.

Unlike the California, Connecticut and Colorado laws, but similar to the Virginia, Utah, and Iowa laws, the INCDPA defines a "sale of personal data," as personal data exchanged for monetary consideration by a controller to a third party but not "other valuable consideration."[14] A sale of personal data under the INCDPA does not include disclosure of personal data: (1) to a processor; (2) to a third party providing services requested by a consumer or a child's parent; (3) to an affiliate of the controller; (4) that a consumer intentionally made available to the public and did not restrict the audience for; or (5) to a third party as an asset that is part of a merger, acquisition or other transaction involving a controller's assets.[15]

The INCDPA also specifies that the above consumer rights do not apply to pseudonymous data where the controller can demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.[16] Additionally, controllers that disclose pseudonymous data must "exercise reasonable oversight" to monitor compliance with any contractual commitments.[17]

The INCDPA grants controllers 45 days to respond to a consumer request, much like other state laws (with the notable exception of Iowa's 90-day response period). This deadline may be extended by an additional 45 days when reasonably necessary, so long as the consumer is informed of the reason behind the extension. Similar to the laws of Iowa, Virginia, Colorado and Connecticut, the INCDPA requires that controllers establish a process for consumers to appeal the refusal to take action on requests to exercise their rights.

What Obligations Do Controllers and Processors Have?

The INCDPA features a similar host of obligations for both controllers and processors as other state privacy laws and the GDPR.

Controller Requirements

- **Data Minimization**: Similar to the Virginia, Colorado and Connecticut laws, controllers must limit collection of personal data to what is adequate, relevant and reasonably necessary in relation to the disclosed purposes for which the data is processed.[18]
- **Data Security**: Controllers are required to establish and maintain reasonable administrative, technical and physical data security practices that are appropriate to the volume and nature of the personal data.[19]
- **Nondiscrimination**: Like other state laws, controllers must not process personal data in violation of state or federal laws against unlawful discrimination against consumers. However, controllers are permitted to offer different prices or discounts if a consumer has opted out of a sale of personal data, targeted advertising or profiling.[20]
- **Processor Agreements**: Similar to other state laws, controllers are required to enter into binding contracts with processors that, among other things, detail the nature and purpose of the processing, instructions for the processing, and the rights and obligations of both parties. Processors under this contract have a number of requirements, such as deleting or returning all personal data to the controller upon the controller's request at the end of the provision of services.[21]
- **Sensitive Data**: Like the Virginia, Colorado and Connecticut laws, controllers must acquire consumer opt-in consent before processing sensitive data. Sensitive data of a known child must be processed in accordance with the Children's Online Privacy Protection Act (COPPA).[22]
- **Transparency and Purpose Specification**: Controllers must provide clear, meaningful and reasonably accessible privacy notices that disclose: (1) the categories of data processed by the controller; (2) the purpose for processing; (3) how consumers may exercise their rights under the law including how to appeal a decision regarding a consumer request; (4) the categories of personal data shared with third parties; and (5) categories of third parties with whom personal data is shared.[23] If a controller is either selling personal data to third parties or using it for targeted advertising, it must clearly

and conspicuously disclose the activity and the manner in which a consumer may opt out.[24]

- **Data Protection Impact Assessment**: Like the California, Virginia, Colorado and Connecticut laws (but unlike the Utah and Iowa laws), controllers must conduct data protection impact assessments for any of the following data processing activities that involve personal data: (1) processing for targeted advertising; (2) selling personal data; (3) processing for purposes of profiling if the profiling presents certain reasonably foreseeable risks;[25] (4) processing sensitive data; and (5) processing activities involving personal data that present a heightened risk of harm to consumers.[26] Importantly, these assessments apply to processing activities that occur **after December 31, 2025**.

Processor Requirements

Similar to other state laws, under the INCDPA processors are required to adhere to controller instructions and assist the controller with their obligations, including (1) responding to consumer requests, (2) implementing appropriate technical and organizational data security measures, (3) notification in the event of a breach, and (4) providing information for data protection impact assessments.[27]

Who Enforces the Law?

The INCDPA does not provide a private right of action and grants exclusive enforcement authority to the Indiana Attorney General (AG). The AG may issue civil investigative demands when the AG has reasonable cause to believe the law has been violated.[28] The AG may seek injunctive relief and civil penalties up to $7,500 per violation, but only after first providing the controller or processor 30 days' notice to cure the violation.[29] Within those 30 days, the controller or processor must provide the AG a written statement that the violations have been cured and no such violations will occur in the future. Similar to the Virginia and Utah laws, this right to cure does not sunset.

The law also gives the AG the option to provide controllers with resources for compliance on its website, including sample privacy notices and disclosures.[30] Given the similarity to other comprehensive state privacy legislation, companies that have complied with earlier state data privacy laws should have little difficulty complying with the INCDPA by its effective date of January 1, 2026.

Learn about the other state laws in Akin's State Data Privacy Law Series, as well as our CCPA Report:

1. Virginia Consumer Data Protection Act: What Businesses Need to Know | Akin (akingump.com)
2. Colorado Privacy Act: What Businesses Need to Know | Akin (akingump.com)
3. Connecticut Data Privacy Act: What Businesses Need to Know | Akin (akingump.com); Businesses and Consumers Prepare as the CTDPA Takes Effect on July 1 | Akin Gump Strauss Hauer & Feld LLP
4. Utah Consumer Privacy Act: What Businesses Need to Know | Akin (akingump.com)
5. Iowa Data Protection Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP
6. Tennessee Information Protection Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP
7. Texas Data Privacy Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP
8. Key Takeaways from Akin's CCPA Litigation and Enforcement Report | Akin (akingump.com)

---

[1] Ind. Code § 24-15-1-1(a) (Indiana 2023).

[2] *Id*. § 24-15-2-19(a).

[3] *Id*. § 24-15-2-28.

[4] *Id*. § 24-15-2-19(b).

[5] *Id*. § 24-15-2-8(b).

[6] *Id*. § 24-15-1-2(1-14).

[7] *Id*. § 24-15-1-2(9-10).

[8] *Id*. § 24-15-1-2(1-13).

[9] *Id.* § 24-15-1-2(3), (8).

[10] *Id.* § 24-15-1-1(b).

[11] *Id.* § 24-15-8-1(a)(1).

[12] *Id.* § 24-15-3-1(b).

[13] *Id.* § 24-15-3-1(b)(4).

[14] *Id.* § 24-15-2-27(a).

[15] *Id.* § 24-15-2-27(b).

[16] Id. § 24-15-7-2.

[17] *Id.* § 24-15-7-3.

[18] *Id.* § 24-15-4-1(1).

[19] *Id.* § 24-15-4-1(3).

[20] *Id.* § 24-15- 4-1(4).

[21] *Id.* § 24-15-5-2(a).

[22] *Id.* § 24-15-4-1(5).

[23] *Id.* § 24-15-4-3.

[24] *Id.* § 24-15-4-4.

[25] *Id.* § 24-15-6-1(b)(3). These are the risks of: unfair or deceptive treatment, unlawful disparate impact, injury that is financial, physical or reputational, physical or other intrusion upon solitude or seclusion or intrusion offensive to a reasonable person, or other substantial injury.

[26] *Id.* § 24-15-6-1(b).

[27] *Id.* § 24-15-5-1.

[28] *Id.* § 24-15-9-1.

[29] *Id.* § 24-15-10-2(a), 3(a).

[30] *Id.* § 24-15-11-2(b).

Categories

Cybersecurity & Information Security

State Privacy Policy

Consumer Data Protection