2026 US Data Privacy Laws Survival Guide

Features + Resources for Each

TABLE OF CONTENTS

Introduction	1
California	2
Colorado	5
Connecticut	8
Virginia	12
Utah	15
Texas	18
Oregon	21
Montana	24
Delaware	27
Iowa	31
Nebraska	34
New Hampshire	37
New Jersey	40
Tennessee	41
Minnesota	46
Maryland	49
Indiana	53
Kentucky	56
Rhode Island	59

TABLE OF CONTENTS

Louisiana	62
Oklahoma	65
Alabama	68
Vermont	71
Additional Resources	74
Preparing for 2026 and Beyond	75

Introduction

The United States doesn't currently have a national comprehensive privacy law, despite efforts to enact one. As a result, U.S. states have been pushed to act independently. The most comprehensive state law is currently lauded by California, and many states are following California's lead by enacting similar or slightly watered-down versions of the CPRA.

All laws are slightly different, however, which can be very challenging for organizations and individuals to navigate. We've distilled the U.S. data privacy law landscape focusing on the key features of each law, demonstrated in the graphic to the right.

Along with these features, we've provided free resources for each law, so you have access to everything in one place.



California

The California Consumer Privacy Act (CCPA) is currently the most comprehensive data privacy law in the United States. It was amended by the California Privacy Rights Act (CPRA).



Effective Dates

- CPRA effective date: 1/1/2023
- CCPA effective date: 1/1/2020
- Enforcement date: 7/1/2023

Resources

Blog: The Expert's Guide to California Data Privacy Law | CCPA & CPRA

Guide: The CPRA Survival Kit

Checklist: 7 Steps to CPRA Compliance:



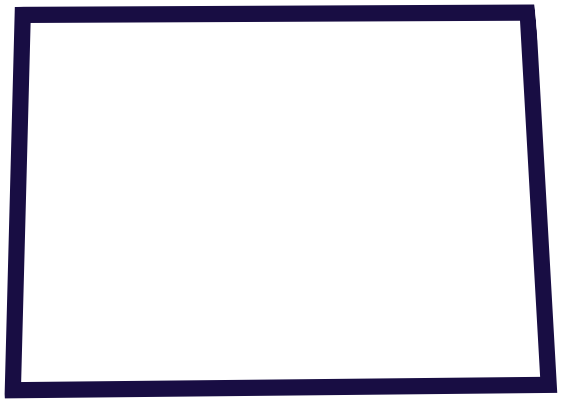
→ **Access Your Copy**

Feature	CCPA Guidelines
Thresholds	• Buys, sells, or shares the personal information of 100,000 people or households. The “shares” part was added with the CPRA, and the number of people was doubled. • Creates 50% or more of your revenue through the sale or sharing of personal information. • Had $25 million in gross revenue in the preceding calendar year. The “preceding calendar year” part was added with the CPRA to make it clear what they meant by $25 million in annual gross revenues.
Fines	• $2,500 per offense for negligent mistakes. • $7,500 per offense for willful offenses.
Cure Period	None
Privacy Impact Assessments	Required for profiling, sensitive data, large-scale processing, and other processing activities with risk of harm to consumers.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	CCPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health condition treatment • Sexual orientation • Sex life • Citizenship/immigration status • Genetic or biometric data for purposes of uniquely identifying an individual • Genetic or biometric data • Precise geolocation • Union membership • Neural data • The personal data of minors under the age of 16
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Sensitive Data) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Limit Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Colorado (CPA)

Colorado was the third state to pass a comprehensive data privacy law, the Colorado Privacy Act (CPA). It's most similar to the CPRA, Virginia's Consumer Data Protection Act, and the GDPR.



Effective Dates

- CPA effective date: 7/1/2023

Resources

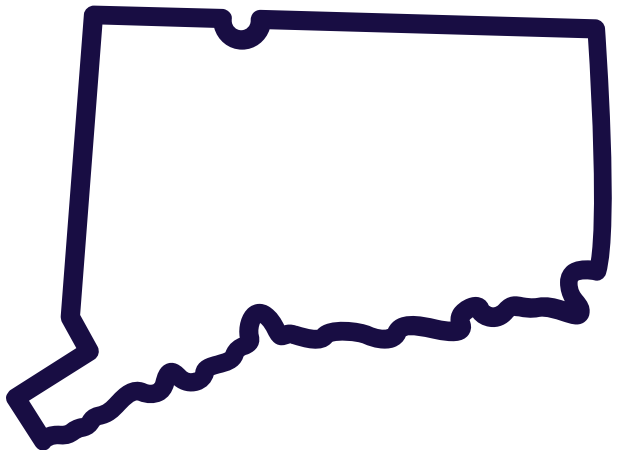
Blog: The Colorado Privacy Act (CPA): Requirements, Enforcement, and More

Feature	CPA Guidelines
Thresholds	• Businesses that collect personal data from 100,000 Colorado residents or • Businesses that collect data from 25,000 Colorado residents and derive a portion of revenue from the sale of that data.
Fines	$20,000 per offense, with penalties capped at $500,000.
Cure Period	Sunsetted on 1/1/2025
Privacy Impact Assessments	Yes
Recognize Universal Opt-Out Mechanisms	Yes

Feature	CPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health diagnosis, condition, and diagnosis made by HCP • Sexual orientation • Sex life • Citizenship or citizenship status • Genetic or biometric data • Personal data of known child • Neural data
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Connecticut (CTDPA)

Connecticut was the fifth state to adopt a privacy law. Known as the Connecticut Data Privacy Act (CTDPA), or “An Act Concerning Personal Data Privacy and Online Monitoring,” Connecticut Bill 6 went into effect on July 1, 2023.



Effective Dates

- CTDPA effective date: 7/1/2023

Resources

Blog: The Connecticut Data Privacy Act (CTDPA): What You Need to Know

Feature	CTDPA Guidelines
Thresholds	Businesses in the state or those that produce products or services targeted to Connecticut residents and who, during the previous year: • Controlled or processed personal data of 35,000 or more consumers, excluding solely for completing a payment transaction • Offer consumers' personal data for sale in trade or commerce • Control or process consumers' sensitive data unless that data is used solely for purposes of completing a payment transaction
Fines	• $5,000 per violation • The Attorney General can also issue orders to offenders to prevent them from violating the law, order disgorgement, and pay restitution to victims.
Cure Period	Sunsetted on 12/31/2024
Privacy Impact Assessments	Required for activities that pose a heightened risk to consumers, such as targeted advertising, the sale of personal data, profiling, processing sensitive data.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	CTDPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health diagnosis, condition, and diagnosis made by HCP • Sexual orientation • Sex life • Citizenship or citizenship status • Genetic or biometric data • Personal data of known child • Precise geolocation • Consumer health data • Status as victim of crime • Consumers' disability or treatment • Status as nonbinary or transgender • Neural data • Financial account numbers, log-in information or credit/debit card number that could allow access to a consumer's financial account • Government-issued identification numbers

Feature	CTDPA Guidelines
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling • Right to Question the Result of Profiling

Virginia (VCDPA)

Virginia's leaders passed The Virginia Consumer Data Protection Act (VCDPA) on March 2, 2021, making it the second state to vote in a comprehensive privacy law after California. As a result, it's similar to the CCPA and the GDPR.



Effective Dates

- VCDPA effective date: 1/1/2023

Resources

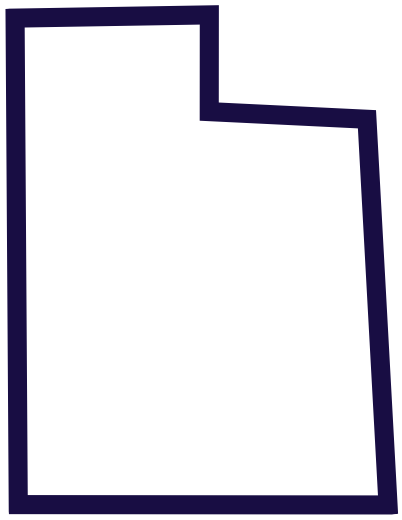
Blog: What Is the Virginia's Consumer Data Protection Act (VCDPA)?

Feature	VCDPA Guidelines
Thresholds	Businesses that sell products and services in Virginia or do so targeting Virginia residents, and also do one of the following: • Control or process the personal data of 100,000 or more; • Control or process the personal data of at least 25,000 consumers and earn 50% of their revenue by selling personal information.
Fines	Up to $7,500 per violation.
Cure Period	30 days, no sunset.
Privacy Impact Assessments	Required for any processing involving targeted advertising, data sales, profiling or sensitive data; or any data processing that presents a "risk of harm."
Recognize Universal Opt-Out Mechanisms	Yes

Feature	VCDPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health diagnosis • Sexual orientation • Citizenship or immigration status • Genetic or biometric data/Genetic or biometric data for purposes of uniquely identifying an individual • Personal data of known child
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Utah (UCPA)

Utah became the fourth state to enact a data privacy law in March of 2022. The Utah Consumer Privacy Act (UCPA) is considered by experts to be more business-friendly than several other privacy regulations in the U.S., including the CPRA, VCDPA, and CPA.



Effective Dates

- UCPA effective date: 12/31/2023

Resources

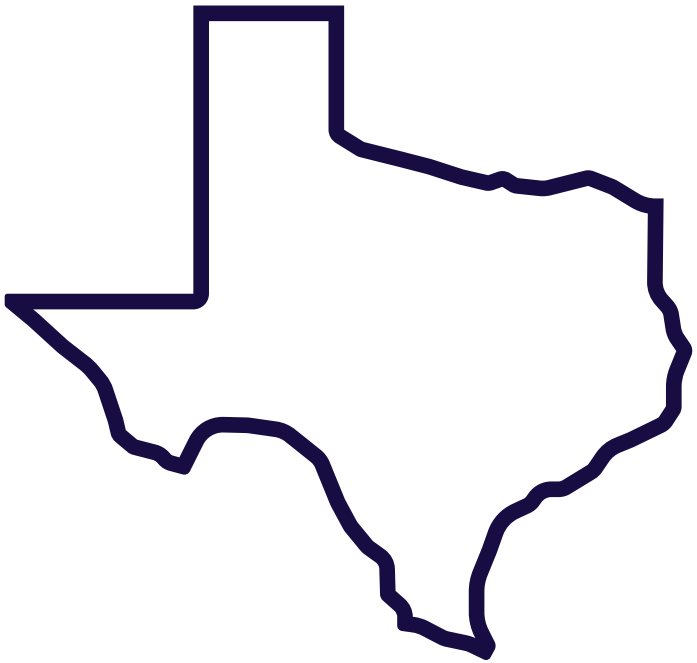
Blog: The Utah Consumer Privacy Act: What Is It, and How to Comply?

Feature	UCPA Guidelines
Thresholds	Have annual revenue of $25m or more AND: • Control/process personal data of 100,000 or more residents, OR • 25,000 or more residents and derive over 50% of gross revenue from selling personal data.
Fines	Up to $7,500 per violation + actual damages
Cure Period	30 days, no sunset
Privacy Impact Assessments	Not required
Recognize Universal Opt-Out Mechanisms	No

Feature	UCPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health condition and medical history, treatment, diagnosis by HCP • Sexual orientation • Citizenship/immigration status • Genetic or biometric data • Precise geolocation
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Delete • Right to correct inaccurate data • Right to Opt Out of Certain Processing (/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Notice and Opt-Out of Sensitive Data Processing

Texas (TDPSA)

The Texas Data Privacy and Security Act (TDPSA) was signed into law on June 18, 2023, making it the largest state in the United States—and the second of the U.S.'s largest states—to have a comprehensive privacy law on the books.



The TDPSA has a few unique aspects, such as the fact that it replaces revenue-based thresholds with a focus on businesses conducting operations in Texas and offering products or services consumed by Texas residents, or businesses that process or sell personal data. It also has a novel small business provision, and while it excludes entities like state agencies and financial institutions, the law does not provide an exemption for organizations governed by HIPAA or GLBA.

Effective Dates

- TDPSA effective date: 7/1/2024

Resources

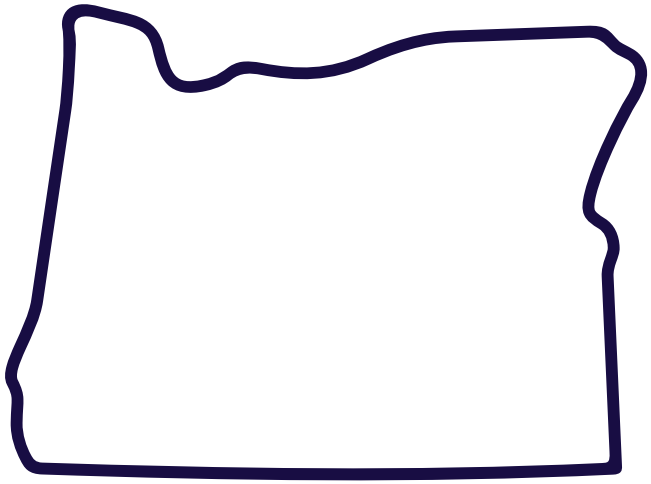
Blog: The Texas Data Privacy and Security Act (TDPSA): All the Basics

Feature	TDPSA Guidelines
Thresholds	• Conduct business in Texas or produce products/ services consumed by residents, OR • Process or engage in the sale of personal data and are not small businesses. There are no revenue thresholds.
Fines	Up to $7,500 per violation and injunctive relief to restrain or enjoin the violator's operations.
Cure Period	30 days, no sunset
Privacy Impact Assessments	Required for targeted advertising, sale of data, profiling, sensitive data processing, other processing activities with risk of harm to consumers.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	TDPSA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health diagnosis, and diagnosis made by HCP • Sexuality • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Oregon (OCPA)

Oregon's legislation passed the Oregon Consumer Privacy Act (OCPA) into law on June 22, 2023. The privacy law is the culmination of four years of work by the Oregon Attorney General's Consumer Privacy Task Force. Other than what's in the chart below, one notable feature is that non-profits aren't exempt from the law. And, like Texas, organizations governed by HIPAA or GLBA are not exempt and must follow OCPA for non-covered data.



Effective Dates

- OCPA effective date: 7/1/2024

Resources

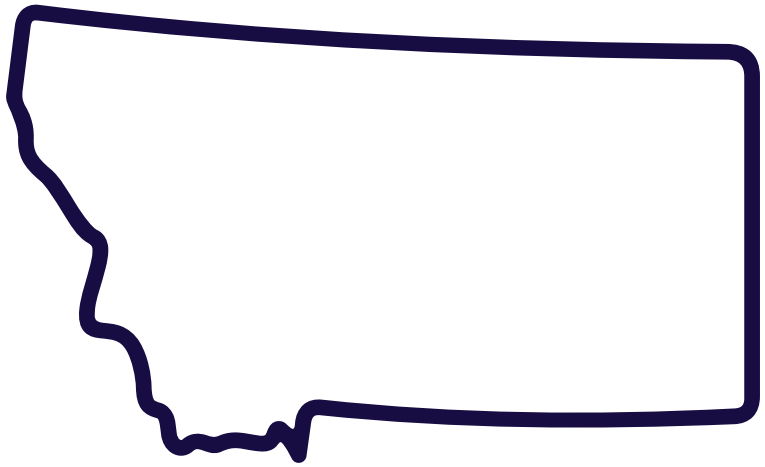
Blog: Oregon's Consumer Privacy Act: The A to Z of the OCPA

Feature	OCPA Guidelines
Thresholds	• Control/process the personal data of 100,000 or more residents, OR • 25,000 or more residents, while deriving 25% or more of gross revenue from selling personal data.
Fines	Up to $7,500 per violation
Cure Period	Sunsetted 1/1/2026
Privacy Impact Assessments	Required for targeted advertising, sale of data, profiling, sensitive data processing, other processing activities with risk of harm to consumers.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	OCPA Guidelines
Sensitive Data	• Racial, ethnic, national origin • Religious beliefs • Mental/physical health condition, diagnosis, medical history and/or treatment, diagnosis by HCP • Sexual orientation and status as transgender/nonbinary • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation • Status as victim of a crime
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to obtain a list of "specific third parties" to whom a controller disclosed personal data • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Montana (MTCDPA)

Montana's governor signed the Montana Consumer Data Privacy Act (MTCDPA) into law on May 19, 2023. The act is similar to data privacy laws in Indiana, Virginia, Colorado, and Connecticut. One unique factor in the MTCDPA is that Montana's thresholds don't only rely on a revenue limit. Find out more in the breakdown below.



Effective Dates

- MTCDPA effective date: 10/1/2024

Resources

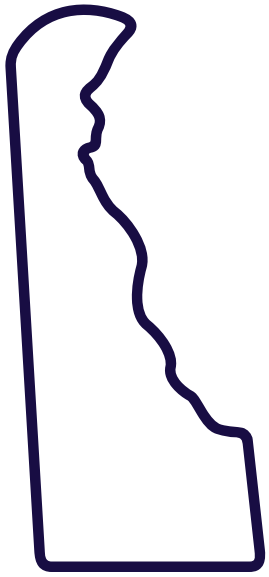
Blog: Discover the Montana Consumer Data Privacy Act—Your Guide to the MTCDPA

Feature	MTCDPA Guidelines
Thresholds	• Control/process the personal data of at least 50,000 residents, OR • 25,000 or more residents and derive more than 25% of gross revenue from selling of personal data. • Duty of care requirements with respect to minors apply to all businesses serving Montanans, save for those explicitly exempted by the law.
Fines	Up to $7,500 per violation
Cure Period	60 days, sunsets 4/1/2026
Privacy Impact Assessments	Required for targeted advertising, sale of data, profiling, sensitive data processing, other processing activities with risk of harm to consumers.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	MTCDPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health condition and/or diagnosis • Sexual orientation, sex life, sexuality • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Delaware (DPDPA)

After the Delaware Personal Data Privacy Act (DPDPA) was voted in, people quickly started lauding it as the strongest data privacy law in the United States. That's not true—California still holds the title—however, it does apply to more businesses than others, and it is one of the more consumer-friendly laws.



Effective Dates

- DPDPA effective date: 1/1/2025

Resources

Blog: What is the Delaware Personal Data Privacy Act (DPDPA): The Basics

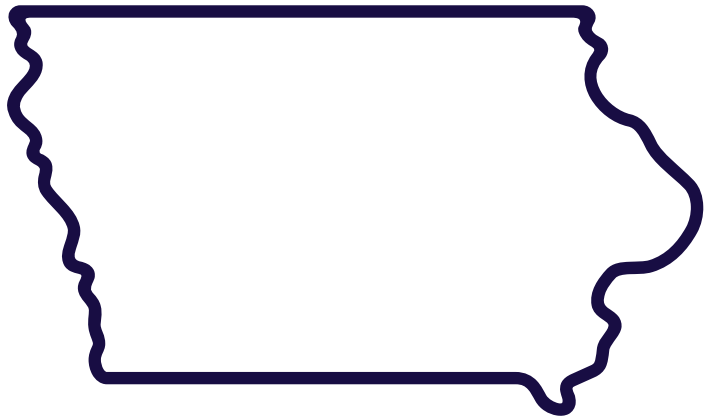
Feature	DPDPA Guidelines
Thresholds	Any company that does business in the state or produces products or services that are targeted to residents of the state and that, during the previous calendar year, met one of the following: • Controlled or processed the personal data of not less than 10,000 consumers (down from 35,000), excluding personal data controlled or processed solely for the purpose of completing a payment transaction. • Controlled or processed the personal data of not less than 5,000 consumers (down from 10,000) and derived more than 20 percent of their gross revenue from the sale of personal data. Also now applies to third parties who acquire personal data from a controller.
Fines	Up to $10,000 per violation, up to the Department of Justice's discretion.
Cure Period	Sunsetted 1/1/2026
Privacy Impact Assessments	Required for targeted advertising, selling personal data, and for profiling if there's a risk of: • Unfair or deceptive treatment to consumers • Financial, physical or reputational injury • Intrusion upon solitude or seclusion (if "offensive to a reasonable person") • Processing sensitive data • Automated decisions with legal/similarly significant effects

Feature	DPDPA Guidelines
Recognize Universal Opt-Out Mechanisms	Yes
Sensitive Data	• Racial, ethnic, national origin • Religious beliefs • Mental/physical health condition, diagnosis, diagnosis by HCP • Sexual orientation and status as transgender/nonbinary • Sex life • Citizenship/immigration status • Genetic, biometric, or neural data • Personal data of a known child • Precise geolocation • Financial info, government ID numbers, and inferences revealing sensitive data

Feature	DPDPA Guidelines
Consumer Rights	• Right to Know/Confirm • Right to Access (incl. inferences) • Right to Obtain a List of Third Parties • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Iowa (ICDPA)

The Iowa Consumer Data Protection Act (ICDPA) was the first comprehensive state privacy law ratified in 2023, making it the sixth overall state privacy law so far. There are a couple of differences in the Iowa law versus the others, such as the lack of provisions for the right to correct PI and the right to opt out of profiling, that it sets a 90-day timeline for responses to subject rights requests, and that it provides businesses with a 90-day cure period as opposed to the 30- or 60-day cure period set by other laws.



Effective Dates

- ICDPA effective date: 1/1/2025

Resources

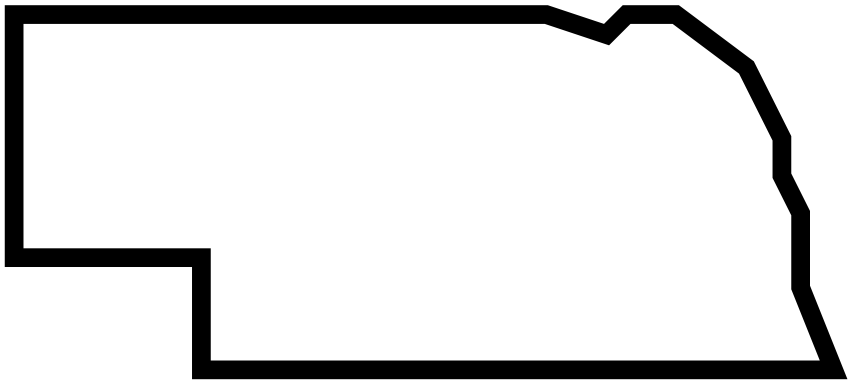
Blog: The Iowa Consumer Data Protection Act (ICDPA): The basics

Feature	ICDPA Guidelines
Thresholds	The law applies to any business that: • Controls or processes the personal data of at least 100,000 Iowa consumers, or • Controls or processes the personal data of at least 25,000 consumers and derives more than 50% of its gross revenue from the sale of personal data.
Fines	$7,500 per violation
Cure Period	Yes, 90 days
Privacy Impact Assessments	ICDPA does not address assessments.
Recognize Universal Opt-Out Mechanisms	No

Feature	ICDPA Guidelines
Sensitive Data	• Racial, ethnic, national origin • Religious beliefs • Mental/physical health diagnosis, diagnosis by HCP • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Delete • Right to Opt Out of Certain Processing (Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt Out of or Limit Sensitive Data Processing

Nebraska (NDPA)

The NDPA is a comprehensive data privacy act designed to protect consumers and give them control over their personal information. It grants them certain rights, outlined below, and provides controllers, or the entity that determines the purpose and means of processing personal data, with specific requirements for how to handle data and consumer requests related to their data.



The law's scope tracks closely with the Texas Data Privacy and Security Act (TDPSA), including its applicability, sensitive data, and its requirement to honor universal opt-out mechanisms.

Effective Dates

- NDPA effective date: 1/1/2025

Resources

Blog: Breaking Down the Nebraska Data Privacy Act: What Businesses Need to Know

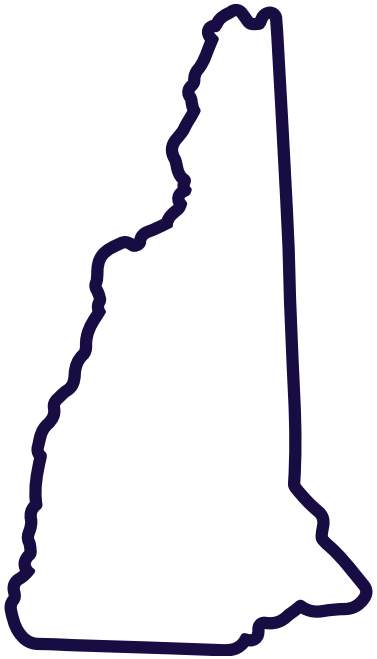
Feature	NDPA Guidelines
Thresholds	Like the TDPSA, Nebraska's privacy law applies to a person who: • Conducts business in the state or produces a product or service consumed by residents of Nebraska; • Processes or engages in the sale of personal data; and • Is not a small business as determined under the federal Small Business Act. One notable aspect of the NDPA's applicability is that, unlike most other state laws, there is no revenue or volume of data processed.
Fines	$7,500 per violation
Cure Period	Yes, if a controller is found to have violated Nebraska privacy act, they have 30 days to cure the violation. Unlike some data privacy acts, the cure period does not have a sunset date.
Privacy Impact Assessments	Required when processing sensitive data; for any processing that involves personal data that presents a heightened risk of harm to any consumer; processing of data for targeted advertising; the sale of personal data; processing for profiling if it presents a risk of impacts like unfair or deceptive treatment, financial, physical or reputational injury, an intrusion on the solitude of a consumer, or other substantial injury to the consumer.

Feature	NDPA Guidelines
Recognize Universal Opt-Out Mechanisms	Yes
Sensitive Data	Like Texas's law, Nebraska's data privacy act defines sensitive data as: • Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; • Genetic or biometric data that is processed for the purpose of uniquely identifying an individual; • Personal data collected from a known child; or • Precise geolocation data.
Consumer Rights	• Confirm whether a controller is processing the consumer's personal data and to access the personal data; • Correct inaccuracies in the consumer's personal data; • Delete personal data provided by or obtained about the consumer; • Obtain a copy of their personal data in a usable format that can be transmitted to another controller; • Opt out of processing for targeted advertising, the sale of personal data, or profiling if the decision would produce a legal or other significant impact on the consumer.

New Hampshire (NHPA)

The New Hampshire Privacy Act (NHPA) is one of a number of statewide data privacy laws aimed at giving consumers control over their personal data in an increasingly digital world.

The good news for businesses is that the NHPA largely resembles other data privacy laws that have come before it.



The New Hampshire data privacy act's scope is somewhat unique in that it doesn't include a revenue threshold. Additionally, the applicability threshold is lower than other laws, but lawmakers have pointed out that this is because of the state's lower population.

Like other U.S. laws, the NHPA follows primarily an opt-out model, meaning businesses are free to process consumer data, but must notify consumers about the processing first and give them a way to opt out of the collection or sale of data.

Effective Dates

- NHPA effective date: 1/1/2025

Resources

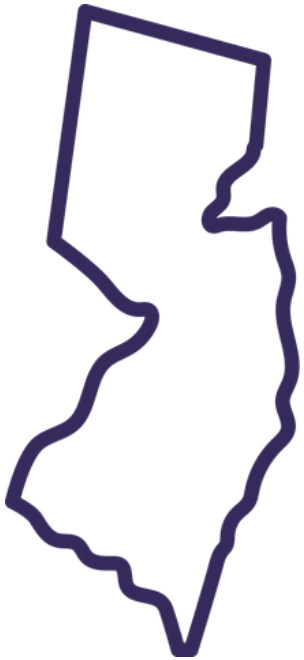
Blog: Understanding the New Hampshire Privacy Act (NHPA): What You Need to Know

Feature	NHPA Guidelines
Thresholds	The NHPA apply to “persons that conduct business” in the state or who produce products or services targeted to residents of New Hampshire and who, during a one-year period: • Controlled or processed the personal data of not less than 35,000 unique consumers, excluding if the processing occurred solely to complete a payment transaction, or • Controlled or processed the personal data of not less than 10,000 unique consumers and derived more than 25 percent of their gross revenue from the sale of personal data.
Fines	The NHPA states that any violations are also a violation of the state’s deceptive trade practices law. This means penalties could be as steep as $10,000 per violation.
Cure Period	Sunsetted 1/1/2026
Privacy Impact Assessments	Required for any processing activity that presents a “heightened risk of harm to a consumer,” including activities such as targeted advertising, sale of personal data, processing for the purposes of profiling in certain instances, and processing sensitive data.

Feature	NHPA Guidelines
Recognize Universal Opt-Out Mechanisms	Yes
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health condition or diagnosis • Sex life • Sexual orientation • Citizenship/immigration status • Genetic or biometric data for the purpose of uniquely identifying an individual • Personal data of a known child • Precise geolocation
Consumer Rights	• Confirm whether a controller is processing the consumer's personal data and access that data • Correct inaccuracies in the consumer's personal data • Delete personal data provided by, or obtained about, the consumer • Obtain a copy of the consumer's personal data processed by the controller, in a user-friendly format • Opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling “in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer”

New Jersey (NJDPA)

The New Jersey Data Protection Act (NJDPA) is a data privacy law that gives New Jersey residents control over their personal data, providing certain rights and imposing obligations on those who control and process consumer data. The law applies to businesses and entities who conduct business in the state or who produce products or services targeted to those who live in New Jersey and meet certain thresholds.



Unlike other state laws, no monetary penalties are defined in the law's text, but a violation of the NJDPA will constitute a violation of the New Jersey Consumer Fraud Act, which can entail fines of up to $10,000 for the initial violation and up to $20,000 for subsequent violations.

Effective Dates

- NJDPA effective date: 1/15/2025

Resources

Blog: The New Jersey Data Privacy Act (NJDPA): The Basics

Feature	NJDPA Guidelines
Thresholds	Applies to controllers who, during a calendar year, meet one of the following criteria: • Control or process the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction, or • Control or process the personal data of at least 25,000 consumers and the controller derives revenue or receives a discount on the price of any goods or services, from the sale of personal data.
Fines	A violation of the NJDPA will constitute a violation of the New Jersey Consumer Fraud Act, which can entail fines of: • up to $10,000 for the initial violation and • up to $20,000 for subsequent violations.
Cure Period	30 days, sunsetting on July 15th, 2026.
Privacy Impact Assessments	• Required for argeted advertising or for profiling if it presents a “reasonably foreseeable” risk of unfair or deceptive treatment of, unlawful disparate impact on consumers, financial or physical injury, physical or other intrusion upon the solitude or seclusion or the private affairs of consumers, or if it would be offensive to a reasonable person. • The sale of personal data. • Processing of sensitive data.

Feature	NJDPA Guidelines
Recognize Universal Opt-Out Mechanisms	Yes
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental or physical health condition, treatment, or diagnosis. • Sex life or sexual orientation • Citizenship or immigration status • Status as a transgender or nonbinary person • Genetic or biometric data that may be process for identifying an individual • Personal data collected from a known child • Precise geolocation data • Financial information
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Opt Out of Automated Decision-Making/Profiling

Tennessee (TIPA)

The Tennessee Information Protection Act (TIPA) was one of three comprehensive state privacy laws signed or ratified in May of 2023. TIPA follows many of its predecessors when it comes to consumer rights, enforcement, and penalties. Unlike its predecessors, however, TIPA diverges by providing a narrower applicability threshold, giving businesses a generous two years to prepare, and implementing an affirmative defense option for those with written privacy programs aligned with specific frameworks such as NIST.



Effective Dates

- TIPA effective date: 7/1/2025

Resources

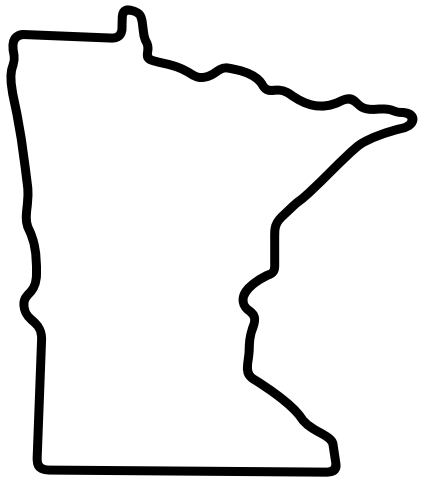
Blog: Tennessee Information Protection Act (TIPA): What to Know

Feature	TIPA Guidelines
Thresholds	TIPA applies to businesses with over $25 million in annual revenue that either conduct business within Tennessee or engage with its residents and either: • Control or process the personal information of at least 175,000 consumers during a calendar year. • Control or process personal information of at least 25,000 consumers and derive more than 50 percent of its gross revenue from the sale of PI.
Fines	• Up to $7,500 per violation • This amount can be tripled if the violations are found to be willful.
Cure Period	60 days
Privacy Impact Assessments	Required for targeted advertising, the sale of personal information, processing sensitive data, processing personal data for profiling, and other processing that may present a heightened risk to consumers.
Recognize Universal Opt-Out Mechanisms	No

Feature	TIPA Guidelines
Sensitive Data	• Racial, ethnic, national origin • Religious beliefs • Mental/physical health diagnosis, condition, diagnosis by HCP • Sexual orientation • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Minnesota (MCDPA)

The MCDPA is a state-level legislation designed to safeguard the personal data of Minnesota residents. Rather than permit organizations to collect, process, and generally do whatever they wish with consumers' personal information, data privacy regulations like the MCDPA set limits on what organizations can do with personal data; require organizations to meet certain obligations, like setting safeguards, assessing for risk, and respecting consumer rights; and provide consumers with data privacy rights that enable them to maintain control over their personal information.



Effective Dates

- MCDPA effective date: 7/31/2025

Resources

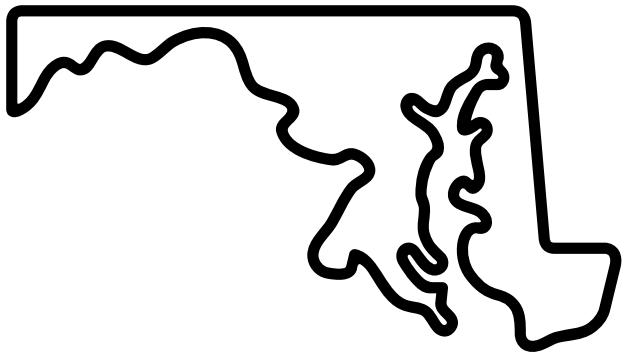
Blog: Everything You Need to Know About the Minnesota Consumer Data Privacy Act (MCDPA)

Feature	MCDPA Guidelines
Thresholds	The MCDPA applies to organizations that provide products or services targeted at Minnesotans and meet one of the following criteria: • During a calendar year, they control or process the personal data of 100,000 consumers or more. • They derive more than 25 percent of gross revenue from the sale of personal data and process or control personal data of 25,000 consumers or more.
Fines	• Up to $7,500 per violation
Cure Period	30 days, sunsetting January 31, 2026
Privacy Impact Assessments	Required for targeted advertising; the sale of personal data; the processing of sensitive data; any processing of personal data that may pose a heightened risk of harm to consumers; and profiling that poses a risk of unfair/deceptive treatment of consumers, injury to consumers, any intrusion on the consumer's solitude, or other substantial injury.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	MCDPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental or physical health diagnosis • Sexual orientation • Citizenship or immigration status • Genetic or biometric data • Data collected from a known child • Specific geolocation data
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Obtain a List of Third Parties • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Question Results of Profiling • Right to Portability/Transfer • Right to Non-Discrimination • Right to Appeal

Maryland (MODPA)

The MODPA gives Maryland residents more control over how companies collect and use their personal data online. With an effective date of October 1, 2025, the new law establishes data protection rights and requires companies that track or target the state's residents to meet stricter requirements around data collection—especially related to data minimization, consent, universal opt-out mechanisms, sensitive data, and children's data. However, MODPA will not apply to companies' data processing activities until April 1st, 2026.



Effective Dates

- MODPA effective date: 10/1/2025

Resources

Blog: What Makes the Maryland Online Data Privacy Act (MODPA) Different?

Feature	MODPA Guidelines
Thresholds	Maryland's privacy law applies to anyone who conducts business in the state, as well as those who provide services or products targeted to residents of Maryland and during the prior calendar year either: • Controlled or processed the personal data of at least 35,000 consumers, with the exception of personal data collected or processed solely for completing a payment transaction, or: • Controlled or processed the personal data of at least 10,000 consumers and derived more than 20 percent of its gross revenue from the sale of personal data.
Fines	Up to $10,000 per violation or $25,000 for each repetition of the same violation.
Cure Period	Discretionary cure period of up to 60 days, sunsetting April 1, 2027.
Privacy Impact Assessments	Required for processing personal data for targeted advertising or selling personal data; processing sensitive data; processing data if there's a risk of unfair, abusive, or deceptive treatment or if it will have an unlawful disparate impact, financial, physical, reputational, or other substantial injury to a consumer; any activity that intrudes on the solitude or seclusion of a consumer. Must be conducted for each algorithm used.

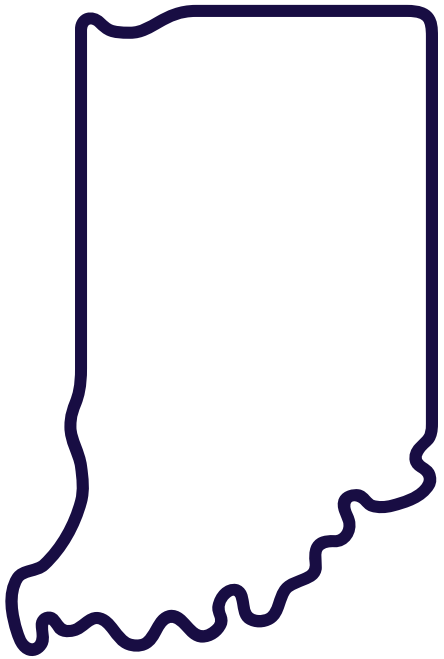
Feature	MODPA Guidelines
Recognize Universal Opt-Out Mechanisms	Yes
Sensitive Data	• Racial or ethnic origin. • Religious beliefs. • Consumer health data. • Sex life. • Sexual orientation. • Status as a transgender or nonbinary. • National origin. • Citizenship or immigration status. • Genetic data • Biometric data • Personal data of a consumer the controller known to be a child • Precise geolocation data

Feature	MODPA Guidelines
Consumer Rights	• Confirm whether a controller is processing their personal data. • Access personal data collected. • Correct inaccuracies in their personal data. • Obtain a copy of the personal data in a portable and readily usable format that provides easy transmission to another controller. • Obtain a list of the categories of third parties to which the controller has disclosed their personal data or a list of third parties to which the controller has disclosed personal data “if the controller does not maintain this information in a format specific to the consumer” • Opt out of the processing of personal data for targeted advertising; the sale of personal data; profiling, if the data is used to make decisions that produce legal or other significant effects

Indiana (INCDPA)

Another of the three state privacy laws to be voted in during May 2023—and the second to do so in 2023 overall—the Indiana Consumer Data Protection Act (INCDPA) is similar to several of its predecessors, including the laws in Colorado (CPA), Connecticut (CTDPA), and Virginia (VCDPA).

Indiana's law, however, does not solely rely on revenue as a threshold—it states that controllers must be compliant with the law even if their annual gross revenues do not meet a specific number as long as the data of a specific number of consumers (outlined in the chart below) is processed.



Effective Dates

- INCDPA effective date: 1/1/2026

Resources

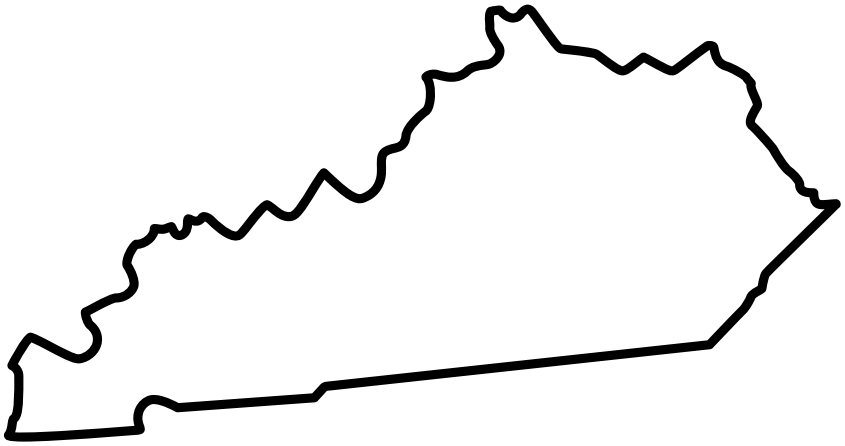
Blog: The Indiana Consumer Data Protection Act: What You Need to Know

Feature	INCDPA Guidelines
Thresholds	Companies that operate in Indiana or sell products and services that are targeted to residents of the state and do one of the following within the previous year: • Control or process the PI of 100,000 residents of Indiana or • Control or process the PI of at least 25,000 residents of Indiana while over 50 percent of your revenue comes from the sale of that PI.
Fines	$7,500 per violation
Cure Period	30 days
Privacy Impact Assessments	Required for the processing of PI for targeted advertising, the sale of personal data, processing sensitive data, processing personal data for profiling with potential risks, and any other processing that may present a heightened risk to consumers.
Recognize Universal Opt-Out Mechanisms	No

Feature	INCDPA Guidelines
Sensitive Data	• Racial, ethnic, national origin • Religious belief • Sexual orientation • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Portability/Transfer • Right to Opt Out of Sales • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Kentucky (KCDPA)

The KCDPA provides data privacy protections for consumers of the Bluegrass State, granting them certain, now standard rights.



The law defines consumers as residents of the state acting only as an individual, not in commercial or employment contexts. It closely aligns with Virginia's law, which is good news for businesses already complying with the Virginia Consumer Data Protection Act (VCDPA). And, because the VCDPA is considered a framework or foundation legislation, the KCDPA also tracks closely with other state laws that used Virginia's law as a framework, including Tennessee and Indiana.

Effective Dates

- KCDPA effective date: 1/1/2026

Resources

Blog: The Kentucky Consumer Data Protection Act (KCDPA): What Businesses Need to Know

Feature	KCDPA Guidelines
Thresholds	The KCDPA applies to any person who conducts business in Kentucky or who produces products or services that target residents of the state, and during a calendar year controls or processes data of at least: • 100,000 consumers; or • 25,000 consumers and derives over 50 percent of gross revenue from the sale of personal data.
Fines	$7,500 per violation
Cure Period	30 days
Privacy Impact Assessments	Required for processing that involves targeted advertising; selling of personal data; profiling, if there is a risk of unfair or deceptive treatment, potential injury to consumers, or an intrusion on their solitude or seclusion; sensitive data; and personal data that presents a heightened risk of harm to consumers. This requirement becomes active June 1, 2026.
Recognize Universal Opt-Out Mechanisms	No

Feature	KCDPA Guidelines
Sensitive Data	The law defines sensitive data as a category of personal data that includes racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data processed for identifying a specific natural person; personal data collected from a known child; or precise geolocation data.
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Opt Out of Certain Processing (Profiling/Targeted Advertising) • Right to Opt out of sale • Right to Portability/Transfer • Right to Opt In for Sensitive Data Processing • Right to Object to Automated Decision-Making/Profiling

Rhode Island (RIDTPPA)

Enacted June 29, 2024, RIDTPPA resembles many other US data privacy laws, including its requirements surrounding consent, sensitive personal information processing, and consumer rights.



The law, however, does feature several important differences, especially regarding its requirements around notices (more on that later).

Notably, the law also lacks a cure period. If you're found to have violated the law, you'll simply be fined without any grace period to fix the violation. Most state data privacy laws feature cure periods, though some expire at various dates in the future, and some are permanent features.

Effective Dates

- RIDTPPA effective date: 1/1/2026

Resources

Blog: All About the Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)

Feature	RIDTPPA Guidelines
Thresholds	Your organization is subject to the RIDTTPA if it is a for-profit entity and conducts business in Rhode Island or provides products or services targeted to Rhode Islanders AND meets one of the following: • Controlled or processed at least 35,000 state residents' personal data. • Controlled or processed at least 10,000 state residents' personal data and derived more than 20% of its gross revenue from the sale of that data.
Fines	$10,000 penalty per violation. If a violator is found to have intentionally disclosed personal information in violation of the RIDTPPA, the state Attorney General can fine the organization between $100 and $500 per violation.
Cure Period	None
Privacy Impact Assessments	Businesses must conduct assessments prior to processing data for targeted advertising, selling personal data, profiling that could pose a risk of unfair or deceptive treatment of consumers; profiling that could cause physical, financial, or reputational injury, intrude on consumers' solitude or private affairs, or cause similar harm; and processing sensitive data.
Recognize Universal Opt-Out Mechanisms	No

Feature	RIDTPPA Guidelines

Sensitive Data	The law defines sensitive data as:
	• Data revealing:
	  ◦ Racial or ethnic origin
	  ◦ Religious beliefs
	  ◦ Mental or physical health conditions or diagnoses
	  ◦ Sex life
	  ◦ Sexual orientation
	  ◦ Citizenship or immigration status
	• The processing of genetic or biometric data for the purpose of uniquely identifying an individual
	• The personal data of a known child
	• Precise geolocation data

Consumer Rights	• Confirm whether a controller is processing their personal data and to access said data • Correct inaccurate personal data • Delete personal data • Data portability • Opt-out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or “profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer”

Louisiana (LDPA)

Louisiana became the 22nd state to enact a comprehensive privacy law when Governor Jeff Landry signed the Louisiana Data Privacy Act (LDPA).



The law borrows its consumer rights and controller obligations from the Texas Data Privacy and Security Act (TDPSA), but its applicability threshold is modeled on California's CCPA—a three-part structure that's uncommon among Virginia-model state laws and can pull in large businesses regardless of how much Louisiana consumer data they actually process.

Effective Dates

- LDPA effective date: 1/1/2027

Resources

Blog: Guide to the Louisiana Data Privacy Act (LDPA)

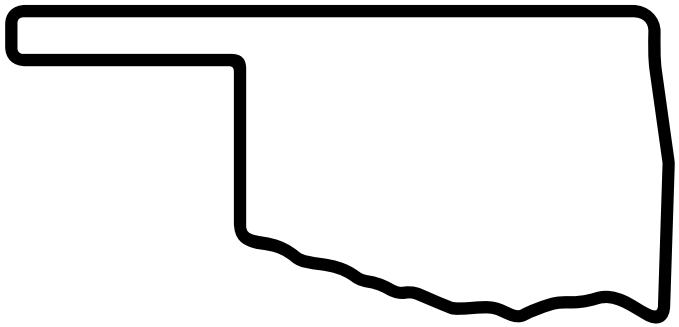
Feature	LDPA Guidelines
Thresholds	• Have annual gross revenues in excess of $25 million; OR • Annually buy, receive for commercial purposes, sell, or share for commercial purposes the personal data of 75,000 or more consumers, households, or devices; OR • Derive 50% or more of annual revenue from selling consumers' personal data
Fines	$5,000 per violation, with up to an additional $5,000 if the violation is committed against an elder person or a person with a disability. Enforced as an unfair/deceptive trade practice under Louisiana's UTPCL—no standalone penalty framework.
Cure Period	30 days; sunsets 7/31/2027
Privacy Impact Assessments	Required for targeted advertising, sale of personal data, profiling with a reasonably foreseeable risk of harm, processing sensitive data, and any other processing that presents a heightened risk of harm to consumers
Recognize Universal Opt-Out Mechanisms	Yes—handled through the law's authorized agent provisions rather than a standalone section. The opt-out signal must be an affirmative, non-default consumer choice.

Feature	LDPA Guidelines
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental or physical health diagnosis • Sexuality • Citizenship or immigration status • Genetic or biometric data processed to uniquely identify an individual • Personal data of a known child • Precise geolocation data (within a 1,750-foot radius)
Consumer Rights	• Right to Know/Confirm • Right to Access • Right to Correct • Right to Delete • Right to Portability/Transfer • Right to Opt Out of Certain Processing (Targeted Advertising/Sale of Data/Profiling)

Oklahoma (OCDPA)

After nearly a decade of legislative attempts, Oklahoma has joined the growing ranks of states with a comprehensive consumer data privacy law, making it the 20th state with such a law on the books.

Modeled closely after Virginia's Consumer Data Protection Act (VCDPA), the OCDPA will feel familiar to privacy professionals who have already navigated the multi-state privacy landscape. That said, like every state privacy law, it has its own nuances.



Effective Dates

- OCDPA effective date: 1/1/2027

Resources

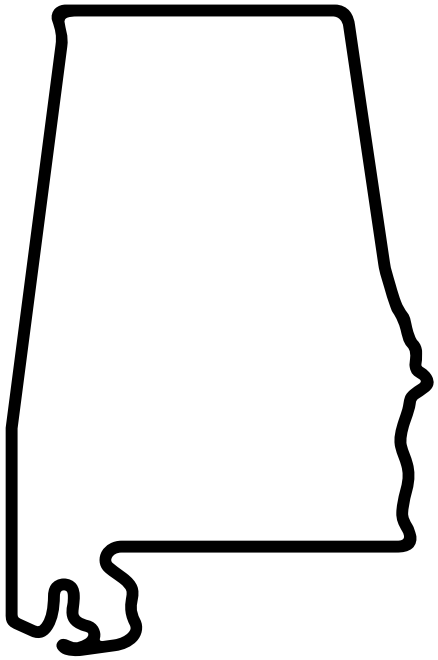
Blog: Oklahoma's Data Privacy Law: What Businesses Need to Know About the Oklahoma Consumer Data Privacy Act

Feature	OCDPA Guidelines
Thresholds	You're subject to the Oklahoma data privacy law if you: • Conduct business in Oklahoma or produce a product or service targeted to Oklahoma residents; and • During a calendar year, either control or process the personal data of at least 100,000 consumers, or control or process the personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data.
Fines	$7,500 per violation
Cure Period	30 days, no sunset
Privacy Impact Assessments	Businesses must conduct assessments for targeted advertising; selling personal data; processing for profiling, where there is a reasonably foreseeable risk of unfair treatment, financial harm, privacy intrusion, or other substantial injury to consumers; processing sensitive data; and any other processing that presents a heightened risk of harm to consumers
Recognize Universal Opt-Out Mechanisms	No

Feature	OCDPA Guidelines
Sensitive Data	The law defines sensitive data as: • Data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status • Genetic or biometric data processed to uniquely identify an individual • Personal data collected from a known child • Precise geolocation data (within a radius of 1,750 feet)
Consumer Rights	• Right to access • Right to correct • Right to delete • Right to data portability • Right to opt out of the processing of their personal data for targeted advertising, the sale of personal data, profiling that produces a legal or similarly significant effect (such as decisions affecting housing, employment, financial services, health care, or access to basic necessities)

Alabama (APDPA)

Alabama has joined the growing list of states with a comprehensive data privacy law. The Alabama Personal Data Protection Act (APDPA) makes Alabama the 21st state to enact a comprehensive privacy framework.



While the APDPA draws most heavily from Virginia's Consumer Data Protection Act (VCDPA), it has plenty of unique features that make it worth studying for businesses seeking to become compliant in either the US as a whole or Alabama specifically. Notable features include a low applicability threshold, a particular "sale" definition that occupies a middle ground across the state privacy law landscape, a higher maximum civil penalty, and the absence of data protection assessment requirements.

Effective Dates

- ADPDA effective date: 5/1/2027

Resources

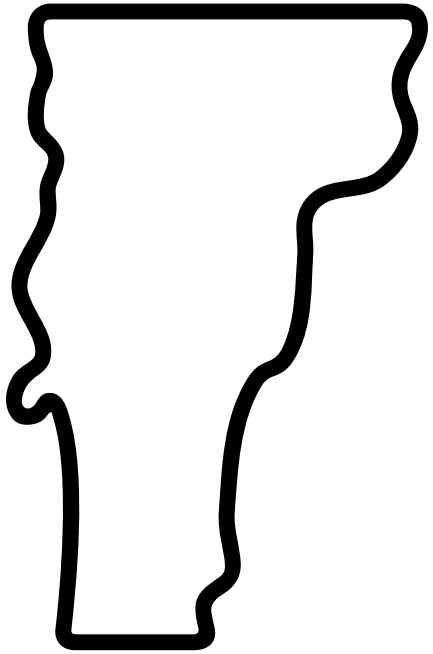
Blog: The Alabama Personal Data Protection Act (APDPA): The US Patchwork Gets Patchier

Feature	APDPA Guidelines
Thresholds	You're subject to the Alabama data privacy law if you conduct business in Alabama or produce a product or service targeted to Alabama residents, and during a calendar year, meet either of the following: • Control or process the personal data of more than 25,000 consumers (excluding data processed solely to complete a payment transaction); or • Derive more than 25% of gross revenue from the sale of personal data, regardless of how many consumers' data you process.
Fines	$15,000 per violation
Cure Period	45 days, no sunset
Privacy Impact Assessments	Not required
Recognize Universal Opt-Out Mechanisms	No

Feature	APDPA Guidelines
Sensitive Data	Sensitive data includes: • Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status • Genetic or biometric data processed to uniquely identify an individual • Personal data collected from a known child • Precise geolocation data (within a radius of 1,750 feet)
Consumer Rights	• Right to access • Right to correct • Right to delete • Right to portability • Right to opt out of the processing of their personal data for targeted advertising, the sale of personal data, profiling in furtherance of solely automated significant decisions, such as credit and lending, housing, employment, and health care decisions and the like.

Vermont (VDPOSA)

Governor Phil Scott signed the Vermont Data Privacy and Online Surveillance Act (VDPOSA) into law on June 16, 2026, after vetoing a stricter version in 2024.



The final version tracks closely with the Connecticut Data Privacy Act, but Vermont layered on several distinctive provisions—including protections for neural data, a dedicated consumer health data section with a geofencing ban, mandatory AI/LLM training disclosures, expanded rights to challenge automated profiling, and a right to name specific third parties that purchased personal data.

Effective Dates

- VDPOSA effective date: 1/1/2028

Resources

Blog: Inside the VDPOSA: Vermont's Unique Take on Data Privacy

Feature	VDPOSA Guidelines
Thresholds	Conducts business in Vermont or produces products/services targeted to Vermont residents, and during the preceding calendar year: • Controlled or processed the personal data of 35,000 or more consumers, excluding payment-transaction-only data, OR • Controlled or processed the sensitive data of 3,000 or more consumers (same payment carve-out), OR • Offered the personal data of 3,000 or more consumers for sale. Note: consumer health data provisions apply to any business doing business in or targeting Vermont, regardless of threshold.
Fines	$10,000 per violation (treated as a violation of the Vermont Consumer Protection Act).
Cure Period	60-day cure period, sunsets 6/30/2029
Privacy Impact Assessments	Required for targeted advertising, sale of personal data, higher-risk profiling, sensitive data processing, profiling for legally or similarly significant decisions.
Recognize Universal Opt-Out Mechanisms	Yes

Feature	VDPOSA Guidelines
Sensitive Data	Sensitive data includes: • Racial or ethnic origin • Religious beliefs • Mental/physical health diagnosis or condition • Sexual orientation • Sex life • Citizenship/immigration status • Genetic or biometric data • Precise geolocation • Personal data of a known child • Neural data • Consumer health data (dedicated section, no-threshold applicability)
Consumer Rights	• Right to know/confirm (including inferences) • Right to access • Right to correct • Right to delete • Right to portability/transfer • Right to opt out of certain processing (targeted advertising, sales, profiling) • Right to question automated profiling results (with correction + reevaluation for housing decisions) • Right to request specific third parties data was sold to • Right to appeal a denied request

Additional Resources

10 Steps to Prepare for 2026

Many of the U.S.'s data privacy laws share common requirements for compliance.

If you tackle the steps in this data privacy compliance checklist in order, you should be in a good place to tailor your privacy program for compliance with the laws that matter most to your organization.



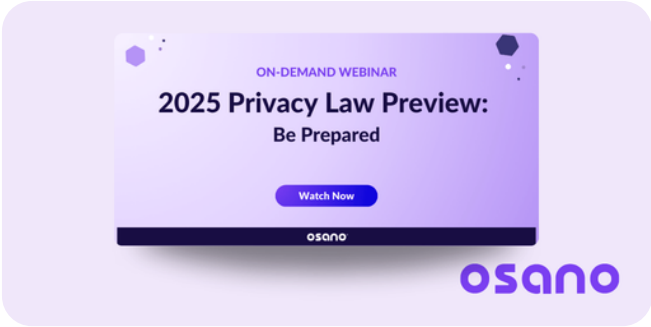
→ **Access Your Copy**

2026's Data Privacy Laws [Webinar]

2026 will see several comprehensive state privacy laws come into effect.

Watch this webinar, with panelists from Osano and Troutman Pepper Locke, as they discuss:

- The essential characteristics of 2026's laws.
- The biggest impact these laws will have on businesses.
- An action plan: what organizations need to do right now to prepare.



→ **Watch On-Demand**

Preparing for 2026 and Beyond

As the data privacy law landscape continues to evolve, it's essential to stay up to date on the latest regulations across the globe in order to avoid fines and penalties while maintaining trust with both your consumers and your team members.

You can learn more about what to expect in 2026 and current developments in the privacy world in the Privacy Insider, a weekly newsletter that covers the latest news in data privacy.

Need Help Complying?

Build the foundation of your organization's compliance processes with Osano.

Schedule a Demo

osano

@osano

linkedin.com/company/osano

http://facebook.com/osanoatx

osano.com

About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.

Copyright © 2024 Osano, Inc., a Public Benefit Corp. Osano is a registered trademark of Osano, Inc.