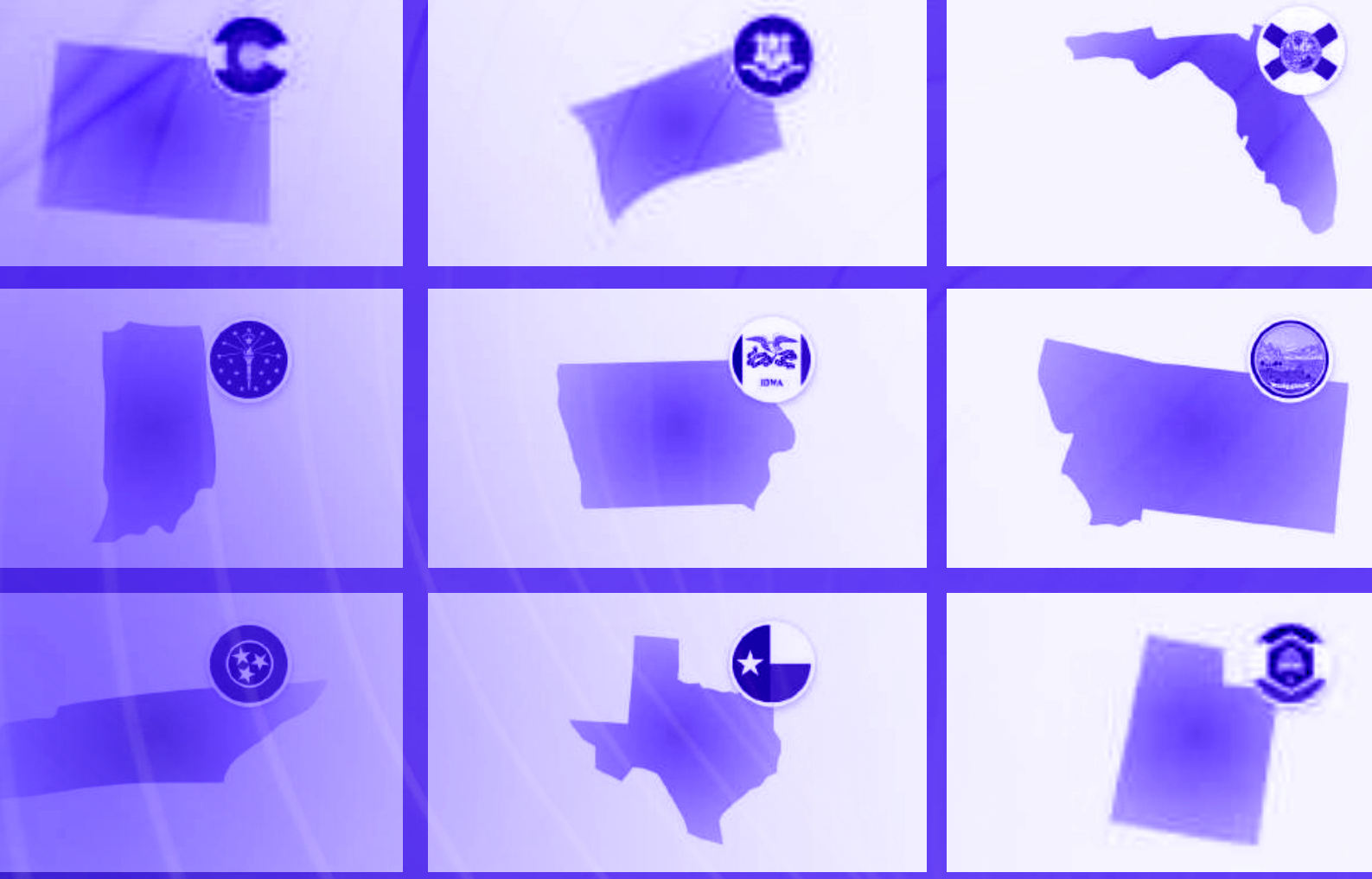


ESSENTIAL GUIDE

The Complete Guide to New

2023 US Data Privacy Regulations

MineOS

intro

2023 is changing the American data privacy scene, with eight states passing comprehensive laws this year alone, joining California, Virginia, Colorado, Connecticut, and Utah to bring the total up to 13 states with comprehensive data privacy regulations.

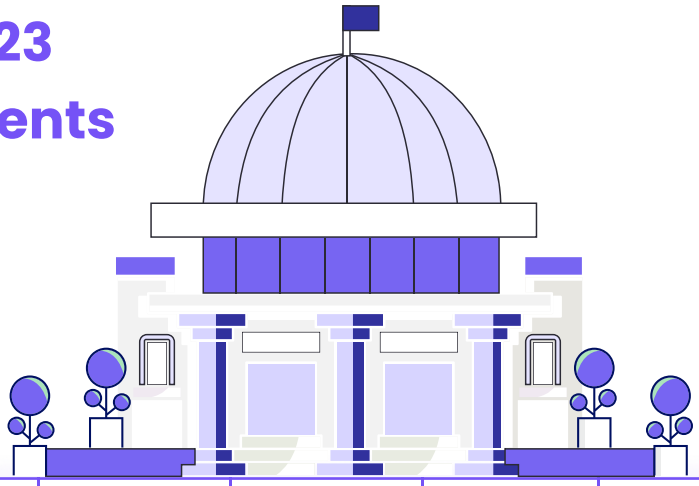
The laws passed and signed into law over 2023 will not all go into effect until 2026, but Iowa, Indiana, Tennessee, Montana, Texas, Florida, Delaware, and Oregon have put themselves on the map and given their citizens protections they absolutely deserve in today's day and age.

Regardless of the future prospects of the ADPPA or another federal bill, more than 135 million Americans–over 40% of the country–now have access to data rights and protections, with that number sure to rise over the next 12 months.

Let's dive into all eight of these new state regulations, highlighting data rights, compliance thresholds, data protection requirements, and unique aspects of each law.

Overview of Overall 2023 Compliance Requirements

*Minus Florida, since it only applies to billion-dollar companies



	Iowa	Indiana	Tennessee	Montana	Texas	Oregon	Delaware
Enforcement Date	January 1, 2025	January 1, 2026	July 1, 2025	October 1, 2024	July 1, 2024	July 1, 2024	January 1, 2025
DPIA	✗	✓	✓	✓	✓	✓	✓
Sensitive Data Processing	Opt-out	Opt-in	Opt-in	Opt-in	Opt-in	Opt-in	Opt-in
Data Minimization & Limits to Secondary Data Use	✗	✓	✓	✓	✓	✓	✓
DSR Response Period	90 days	45 days	45 days	45 days	45 days	45 days	45 days
Right to Revoke Consent	✗	✗	✗	✓	✗	✓	✓
Fines	$7500	$7500	$7500	$7500	$7500	$7500	$10000
Cure Period	90 days Permanent	30 days Permanent	60 days Permanent	60 days Ends 4/1/26	30 days Permanent	30 days Ends 1/1/26	60 days Ends 1/1/26

Iowa Consumer Data Protection Act

Enforcement Date: **January 1, 2025**

Iowa passed its regulation, the Iowa Consumer Data Protection Act (ICDPA) quickly and with broad–nearly unanimous–support from the state's legislature. It was the first state to pass data privacy regulation in 2023 and just the second Republican-led state to (after Utah) to do so, giving the legislature a strong bipartisan win.

Iowa used Virginia's VCDPA as a basis for much of its bill, so there is immense overlap between the two, including the ICDPA's fines of $7500 per violation and its applicability threshold for businesses processing:

- the personal data of +100,000 consumers in a calendar year, or
- the personal data of +25,000 consumers, while deriving over 50 percent of gross revenue from the sale of that data.

Despite that, the actual contents of the ICDPA leave much to be desired. Consumer data rights only include:

Consumer Rights

- Confirm
- Access
- Delete
- Portability
- Appeal

This means that Iowans will lack major data rights like the right to correct data, the right to revoke consent, and the right of private action.

ICDPA also relies almost entirely on opt-outs, with even the processing of sensitive data as an opt-out rather than opt-in for individuals.

Iowa Consumer Data Protection Act

The bill also does not grant the right to opt out of profiling or the use of personal data for targeted advertising, two major issues that have routinely been the focus of recent GDPR fines in the EU.

The age of a child for opt-in purposes is 13, the same as the federal Children's Online Privacy Protection Act (COPPA). Only children under 13 have opt-in rights under the ICDPA.

Iowa also grants businesses the longest timeline for handling data subject requests of any comprehensive state-level bill in America, as they have 90 days to respond to DSRs rather than the 45-day limit in the CCPA and VCDPA.

This is on top of a 90-day cure period that will not expire, meaning businesses have a very long runway for fixing any alleged violations.

Notable Exemptions

- Government bodies
- Non-profits
- Higher education
- Employment-related data
- Entities subject to GLBA
- Entities subject to HIPAA
- Farm Credit Act

Things to note

- **The 90-day cure period is permanent**
- **Iowa's bill is the only comprehensive bill to pass this year that does not require businesses to conduct impact assessments, which is why the ICDPA has arguably the lowest overall bar for compliance**
- **The bill makes no mention of the Global Privacy Control or other universal opt-out mechanisms**

Indiana Consumer Data Protection Act

Enforcement Date: **January 1, 2026**

Indiana's comprehensive data privacy regulation (INCDPA) has the latest enforcement date of the eight bills passed in 2023, with the state granting businesses a grace period of more than two and a half years from the time the regulation passed.

Grace period aside, Indiana follows the VCDPA closer than Iowa's law does, granting its residents these data rights:

Consumer Rights

- Confirm
- Access
- Correct
- Delete
- Portability
- Opt-out of sales, targeted ads, & profiling
- Appeal
- Opt-in before a data controller can process sensitive data

The only major data right missing is the right of private action, which means individuals are not allowed to sue organizations over data privacy violations. However, this data right is absent from nearly every American regulation sans California's CCPA, so its exclusion here is not surprising.

In addition to consumer-friendly benefits like requiring businesses to receive opt-in before processing sensitive data, Indiana requires impact assessments and calls for "adequate" data security measures, as well as data protection principles like data minimization and transparency.

It's applicability threshold is the same as Virginia's & Iowa's:

1. control or process personal data of at least 100,000 consumers or
2. control or process the data of 25,000 consumers while also making over 50% of gross revenue from the sale of personal data.

Indiana Consumer Data Protection Act

Exemptions

- Government
- Non-profits
- Higher education
- Public utilities
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Children's Online Privacy Protection Act (COPPA)
- Data covered by the Health Care Quality Improvement Act
- Data covered by the Patient Safety and Quality Improvement Act
- Data covered by the Fair Credit Reporting Act
- Data covered by the Driver's Privacy Protection Act
- Data covered by the Family Educational Rights and Privacy Act
- Data covered by the Farm Credit Act

This is the full list of exemptions for the INCDPA, but the vast majority of these apply to all the state privacy laws within America; for that reason, we won't be reposting the full list for every law

Things to note

- **Permanent 30-day cure period (similar to Virginia, but differing from Colorado & Connecticut, both of which have a sunset cure period that will expire before Indiana's bill even takes effect in 2026**
- **Indiana's DSR handling timeline matches California's, with 45 days to respond and address consumer requests**
- **The bill makes no mention of the Global Privacy Control or other universal opt-out mechanisms**

Tennessee Information Protection Act

Enforcement Date: **July 1, 2025**

The Tennessee Information Protection Act (TIPA) passed in early May, and shares many things previous state laws, including a standard 45-day timeline to respond to DSRs and Attorney General-led enforcement, with fines of $7500 per violation

TIPA's applicability threshold takes Utah's approach, as companies only need to comply if they:

1. Earn more than $25 mil in gross annual revenue **AND**

A) control or process personal information of +175,000 Tennessee consumers **OR**

B) control or process personal information of +25,000 Tennessee consumers while making +50% of revenue from the sale of that data.

This law only covers people acting in "a personal context," which means employees and business-to-business data are not covered by the law. Currently the only state law that extends full rights to employees is California's CCPA.

Tennessee requires companies to secure opt-ins before processing any sensitive data or data from a known child under the age of 13. Otherwise, TIPA works on opt-outs, although it does grant consumers the ability to opt-out of data processing for profiling and targeted advertising.

Consumer Rights

- Confirm
- Access
- Correct
- Delete
- Portability
- Opt-out of sales, targeted ads, & profiling
- Appeal
- Opt-in before a data controller can process sensitive data

Tennessee Information Protection Act

TIPA has a long list of exemptions, exempting all the categories listed in Indiana's law with one difference: public utility companies are not exempt, but instead licensed insurance companies are.

TIPA is currently the only bill that exempts insurance companies, which is something that often pops up in state bills as key industries within a state secure additional guarantees from data privacy regulations.

The other unique aspect of TIPA is a section outlining a safe harbor for companies that "reasonably conform" to the NIST Cybersecurity Framework. While NIST's framework is just a guideline, it is quite influential, outlining how companies should cover risks in how they Identify, Protect, Detect, Respond, and Recover data.

What this safe harbor defense actually looks like in practice is anyone's guess, but in theory it could mean companies that have industry standard cybersecurity practices in place have a defense if they are found to be in violation of TIPA.

The first time this comes up, the fabric of TIPA will be tested and the country will be watching given how unique this clause is.

Things to note

- **TIPA has a permanent 60-day cure period**
- **Companies do not need to include pseudonymous data when fulfilling DSRs**
- **Impact assessments are required, and companies will need to begin documenting data processing activities by July 1, 2024–one year before the law enters into effect**

Montana Consumer Data Privacy Act

Enforcement Date: **October 1, 2024**

Montana's law, the Montana Consumer Data Privacy Act (MCDPA), was drafted in late 2022 and passed a week after TIPA in May. Despite coming after Iowa, Indiana, and Tennessee, Montana's law enters into force before any of them.

The MCDPA's applicability thresholds are also lower than any state to pass data privacy regulation in 2023 and do not specify a revenue threshold, with companies needing to comply if they:

1. Control or process personal information of +50,000 Montana consumers

OR

2. Earn +25% of gross revenue from the sale of personal data and control and/or process the personal data of +25,000 Montanans

The 50,000 mark is half what most states have on the books, which is logical given Montana's small population. Like the other laws in 2023, employees are not covered by MCDPA.

Consumer Rights

- Confirm
- Access
- Delete
- Portability
- Appeal
- Correct
- Revoke Consent
- Opt-out of sales, targeted ads, & profiling
- Opt-in before a data controller can process sensitive data

Montana becomes just the second state after Connecticut to give citizens the right to revoke consent within the original regulation (Colorado amended theirs to include the right to revoke consent).

Montana Consumer Data Privacy Act

Likewise, the MCDPA allows people to request that data controllers delete all personal data the controller has on them, rather than just personal data that the controller collected directly from the consumer, which is not the standard for data subject rights. The bill also does not require Montanans prove their identity to opt-out of targeted advertising and the selling of their personal data, making opt-outs simpler and faster.

One more edge is that consumers must be able to opt-out of the sale of personal data for the purpose of targeted advertising by January 1, 2025 (3 months after the law enters into force).

Despite operating on an opt-out principle for data processing, sensitive data will require opt-in consent, which is becoming the norm for state-level bills, with these categories covered by the MCDPA and most regulations:

Categories of Sensitive Data

- racial/ethnic origin
- religious beliefs
- mental or physical health diagnoses
- sexual orientation
- citizenship or immigration status
- data from a known child (≤13 years old)
- genetic or biometric information used to uniquely identify an individual
- precise geolocation data (within a radius of 1,750 feet)

Things to note

- **DSR timeline is 45 days, like most other American regulations**
- **Children are defined as under 13 years old, but there are extra protections in place for those under 16, as consent is required if data processing is for the sale of data or targeted advertising.**
- **The usual nationwide exemptions apply**
- **Data minimization, data security standards, and impact assessments are required**
- **60-day cure period set to expire on April 1, 2026**

Florida Digital Bill of Rights

Enforcement Date: **July 1, 2024**

Technically, Florida became the tenth state to pass comprehensive data privacy regulation in June when Governor DeSantis signed the Florida Digital Bill of Rights (FDBR) into law, but the law's scope is so limited many legal outlets have not spent much time covering it.

The FDBR defines data controllers as an organization with annual global revenue of over $1 billion, almost immediately limiting the law's applicability threshold to Big Tech and the most high-profile advertising companies (the usual exemptions for health care and financial institutions apply).

That leaves the applicability threshold as such:

- Make an annual revenue of +$1 billion in a calendar year
  AND
- Make 50% of annual revenue from selling online ads
- Run an app store or digital distribution platform that has over 250,000 downloadable apps for consumers
  OR
- Sell a smart device that comes equipped with a virtual assistant or voice command service

With that picture in place, it becomes clear that Florida is exclusively trying to regulate specific companies like Google, Amazon, and Apple.

The bill takes particular aim at smart home devices and social media, as it requires companies to gain clear consent before any device that uses voice or facial recognition, video, audio, or other monitoring capabilities begins operation.

Florida Digital Bill of Rights

In regards to social media, the bill bans government entities from signing content moderation agreements with social media platforms, as has occurred previously with Twitter and Meta.

FDBR also takes aim at search engines, specifically Google, requiring it to provide clear insight into how its algorithms and methodology work, including disclosing how factors such as political ideology and partisanship is handled within search results.

These are the restrictions on and requirements of data controllers:

FDBR Compliance Requirements

- Practice data minimization, only collecting what is necessary for the stated purposes
- Implement and maintain adequate data security measures
- Obtain consumer consent before processing sensitive data, the categories of which the state expanded to now include geolocation and biometric data
- Follow strict data retention schedules, not exceeding two years after a consumer's last interaction with the controller or beyond the end of a data processing contract
- Conduct data protection impact assessments

Unlike other state laws, the FDBR applies to any company whose products are used by Florida residents. This is a slight difference in language, as most states specify products and services aimed at state residents or a company located within a state.

That means Big Tech companies will need to comply with the FDBR by default, which is a feature of the bill, since it will likely only cover a few dozen companies globally.

Florida Digital Bill of Rights

Consumer Rights

- Confirm
- Access
- Delete
- Opt-out of sales, targeted ads, & profiling
- Appeal
- Correct
- Portability
- Opt-in before a data controller can process sensitive data

Things to note

- **Enforcement is handled completely differently in Florida, led not by the AG but by the Florida Department of Legal Affairs. This, in theory, means more resources to prosecute violations, particularly with only an optional cure period provided**
- **Violations carry a $50,000 fine per occurrence, with that number reaching $150,000 if the violation involves a child's data**
- **Children are defined as under the age of 18, and have increased protections put in place for "online platforms." Online platforms are prohibited from processing the personal information of children if the platform's data processing poses a substantial risk or harm to children's privacy**
- **DSR response timeline is the normal 45 days**

Texas Data Privacy & Security Act

Enforcement Date: **July 1, 2024**

Texas passed the Texas Data Privacy & Security Act (TDPSA) shortly after Florida, becoming the sixth state in 2023 and 11th overall to pass comprehensive data privacy regulations.

Unlike Florida's FDBR, Texas's law follows the standards set by other state regulations like the VCDPA more closely, but there are some deviations. The main difference is the TDPSA's applicability threshold, which requires businesses to meet these three criteria:

- Conduct business in Texas or offer a product or service consumed by Texas residents
- Process or engage in the sale of personal data
- Is not a small business as defined by the U.S. Small Business Administration *(500 employees or fewer, revenue under $30 million)*

This is perhaps the broadest applicability threshold of all the state-level data privacy laws, and takes the opposite approach Florida took. The TDPSA looks primed to require many businesses to comply, even if the U.S. Small Business Administration definitions vary in size and revenue thresholds by industry.

The one overlap with Florida's threshold is the phrasing about a company offering products or services "consumed" by Texans being subject to compliance.

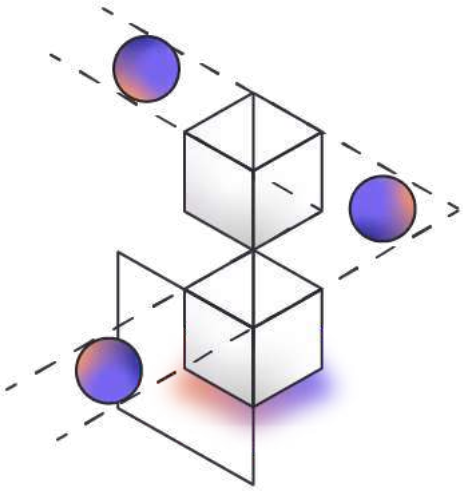
This opens the door for nearly any company operating within the United States and bringing in over $30 million (similar to the $25 million revenue threshold in California's CCPA) to comply, possibly setting a more national standard for how companies handle data privacy within the country.

Texas Data Privacy & Security Act

Like most states, Texas's law includes quite a few exemptions:

- State government and administrative organizations
- Institutions and data subject to the Gramm-Leach-Billey Act (GLBA)
- Entities, associates, and data covered by HIPAA
- Nonprofit organizations
- Higher education institutions
- Electric utility and power generation companies**
- Data related to the Health Care Quality Improvement Act of 1986
- Data in compliance with the Driver's Privacy Protection Act of 1994
- Data in compliance with the Family Educational Rights and Privacy Act of 1974
- Data in compliance with the Farm Credit Act of 1971

The one unique exemption is for electric utility and power generation companies. This is key for Texas as it is the only state in the country to run on its own power grid, hence why the state is more lenient to those companies.



Texas Data Privacy & Security Act

Texas residents will soon get data rights including the right to access, delete, correct, data portability, and opt-out of targeted advertising and automated profiling. The TDPSA does not include the right of private action or the right to revoke consent.

Of note regarding the right to access, Texas has a unique clause whereby data controllers must include special clauses noting if they sell a consumer's sensitive or biometric data.

Data subject requests will operate on the typical 45-day timeline and companies must conduct data protection assessments that cover:

- Targeted advertising
- Selling or sharing personal data
- Automated profiling and decision making
- Processing sensitive personal information
- Activities that present a "heightened risk of harm to the consumer"

Things to note

- **Processing sensitive information requires a freely given opt-in**
- **The law calls out dark patterns as defined by the FTC in how consent notices must be written**
- **Organizations must acknowledge and honor universal opt-out systems by January 1, 2025**
- **30-day indefinite cure period, although businesses must include evidence of compliance and correction of alleged violations when given written notice by the AG instead of simply responding that they have corrected the violation**

Oregon Consumer Privacy Act

Enforcement Date: **July 1, 2024**

Oregon passed the Oregon Consumer Privacy Act (OCPA) in July, the second most recent state to pass a data privacy law in the U.S. The OCPA is not radically different from the bulk of state-level data privacy regulations currently out there, a mild surprise given how progressive a state Oregon is, but the law has its own special facets.

Firstly, the applicability threshold does not have a revenue requirement, applying to any business within the state or producing services targeted at state residents that:

- controls or processes personal data of +100,000 Oregon residents, **OR**
- controls or processes personal data of +25,000 Oregon residents and earns more than 25 percent of gross revenue from the sale of personal data.

As for exemptions, the usual ones are present here (government entities, higher education, HIPAA or GLBA-covered entities, health records, research data, etc.), but there is one major change.

Non-profits within Oregon are NOT exempt from the OCPA, meaning they too must comply. Oregon is only the second state after Colorado to require compliance from most non-profit organizations. Non-profits will have an extra year, until July 1, 2025, to comply.

Consumer Rights

- Confirm
- Access
- Delete
- Portability
- Appeal
- Revoke Consent
- Correct
- Opt-out of sales, targeted ads, & profiling
- Opt-in before a data controller can process sensitive data

Oregon Consumer Privacy Act

The DSR handling timeline for businesses in compliance with OCPA is 45 days, but one interesting wrinkle is that consumers also have the right to appeal a data controller's refusal to handle a data subject request.

As just the fourth state to include the right to revoke consent and one of the very few to include the right to appeal, Oregon consumers may enjoy the strongest set of data rights in the country.

Compliance requirements for businesses cover the usual points such as data minimization, adequate data security standards, guardrails to stop discrimination against individuals exercising their data rights, transparent consent and privacy notices, and the need to carry out impact assessments.

The state goes further with requirements however, as data controllers and processors must sign and carry out agreements on how to process data (not required by every state), and controllers must disclose to consumers how third parties might process the data shared with them.

Things to note

- **The processing of sensitive data requires opt-in, and processing any data of children under 13 also requires opt-in**
- **Additional protections for children aged 13-15, as data controllers must get explicit consent before processing data for targeted advertising, selling personal data, or profiling.**
- **Extensive third party disclosures go beyond the mere listing of data categories potentially shared with third parties most regulations require**
- **$7500 fine per violation, with AG-only enforcement**
- **30-day cure period that ends January 1, 2026**

Delaware Personal Data Privacy Act

Enforcement Date: **January 1, 2025**

Delaware passed the Delaware Personal Data Privacy Act (DPDPA) in September, becoming the eighth state in 2023 to pass a comprehensive data privacy law and the lucky 13th state overall.

Delaware's approach to an applicability threshold eschews a revenue threshold, with businesses either within the state or producing goods and services targeted at Delaware residents needing to comply if during a calendar year they:

- control or process personal data of +35,000 Delaware residents
  OR
- control or process personal data of +10,000 Delaware residents while earning more than 20 percent of gross revenue from the sale of personal data.

These numbers are far below the normal 100,000 figure, as Delaware–like Montana–has quite a small population. The 20% of revenue earned from the sale of data is below the normal 25% figure, another fact to note.

The law's exemptions cover government entities, HIPAA-related data, GLBA-covered entities, health records, research data, etc. but most non-profits and higher education institutions are NOT exempt.

The two important differences here are the fact that the state exempts only HIPAA-related data and not a broader HIPAA-related entity exemption that most states have, and the fact that Delaware is the first state to require higher education institutions to comply with its comprehensive data privacy regulation.

Delaware Personal Data Privacy Act

Consumer Rights

- Confirm
- Access
- Delete
- Portability
- Appeal
- Correct
- Opt-out of sales, targeted ads, & profiling
- To see which third parties a controller has shared the specific consumer's data with (a right only also in the OCPA)

Also like Oregon, Delaware also offers the right to appeal a controller's refusal to take action on a data subject request, but the state lacks the right to revoke consent (as well as the right of private action, meaning California is still the only state to grant citizens that right).

Along with normal requirements placed on data controllers like data minimization, contracts between data controllers and processors, data security standards, etc. Delaware's DPDPA of course requires impact assessments.

However, any company processing the data of over 100,000 consumers within Delaware (population 1.01 million) must conduct and document data protection impact assessments on "a regular basis."

For larger companies, this likely means stricter privacy program controls than are currently in place, which will hopefully spur many in the business world to invest more heavily in data privacy.

Delaware Personal Data Privacy Act

Delaware, as the most recent state to pass regulation, has extended the definitions of various sections within the DPDPA. Most notably, it expands the right to opt-out of profiling to also cover “demographic characteristics” and becomes the first state to include “status as transgender or nonbinary” as part of sensitive information.

However since the law does not cover business-to-business or employee information (like all the other 2023 bills), people will still see demographic questions when applying for jobs.

Delaware also has some of the most stringent restrictions on processing children’s data.

Children are defined as under 13 years of age and processing any data from a child requires explicit opt-in and parental consent, but the DPDPA also partially covers kids under 18 years old, as data controllers must not sell or process their personal data for targeted advertising without consumer opt-in.

Things to note

- **DPDPA enforcement looks different from most states’ data privacy enforcement, as fines reach $10,000 per violation and enforcement is carried out not only by the AG, but by the entire Delaware Department of Justice.**
- **60-day cure period until January 1, 2026, upon which the cure period becomes optional to provide**
- **Controllers will need to recognize universal opt-out mechanisms starting January 1, 2026.**

outro

As you can see, 2023 has been an incredibly busy year for American data privacy and data privacy laws in the U.S.

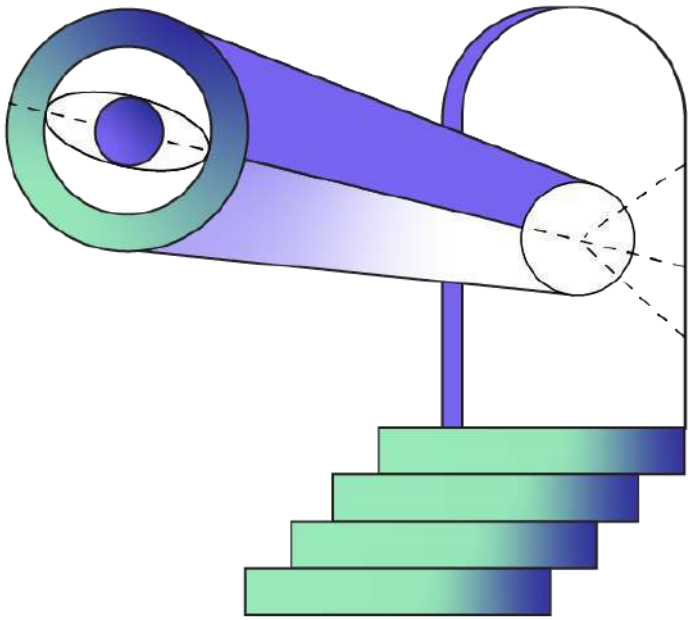
To go from five to 13 states with comprehensive laws on the books is a major win for data privacy and data rights. As most of these states were able to pass their respective regulations within a single legislative session, there is real momentum and urgency behind the issue now.

In 2024, several more states seem primed to pass comprehensive data privacy laws, with New Hampshire looking to be next in line at the beginning of the 2024 legislative session.

Keep your eyes here as we will update the guide with each new passing state regulation, making it a perfect in-depth companion to IAPP's legislation tracker.

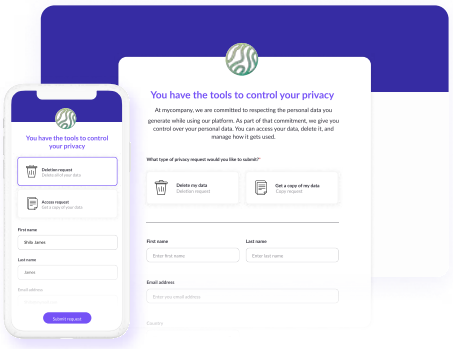
As a reminder, this is the timeline for these eight new laws to enter into effect:

- July 1, 2024 – Oregon
- July 1, 2024 – Florida
- July 1, 2024 – Texas
- October 1, 2024 – Montana
- January 1, 2025 – Iowa
- January 1, 2025 – Delaware
- July 1, 2025 – Tennessee
- January 1, 2026 – Indiana

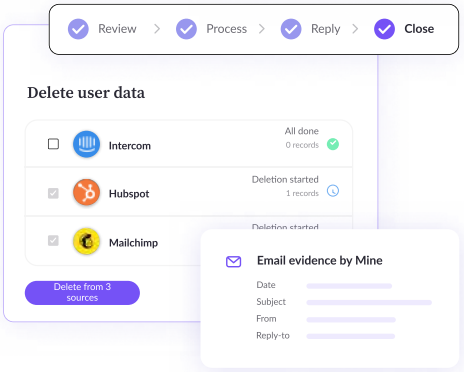


How MineOS Helps You Manage Privacy

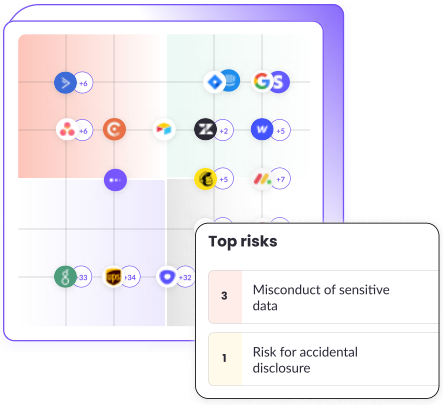
Try MineOS



Connect your DSR channels including email, phone, API and our own embeddable, customizable Privacy Center form.

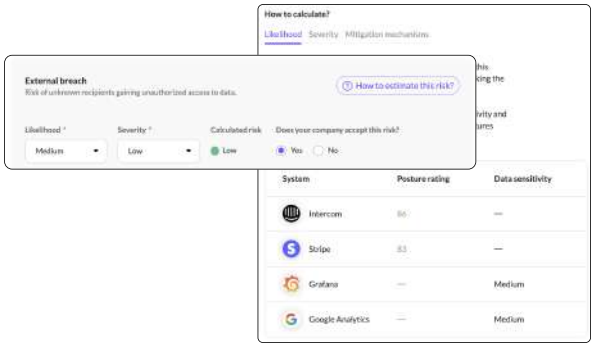


Track and handle incoming DSRs automatically with our hundreds of integrations and seamless one-click workflows.



Automatically collate information from our email discovery with cybersecurity metrics (via our partner Panorays) to understand where risks are.

Use our metrics, tips and intuitive DPIA interface to easily build a thorough accounting of risk likelihood, severity and mitigation mechanisms.



The Privacy Platform for You

Prepared for all the new data regulation requirements? It's harder than ever in today's landscape, which is why most companies need to nail their choice of privacy platform.

MineOS's full privacy management suite gives companies powerful yet easy-to-use tools that don't take months to get going, so you can manage compliance and build a privacy program that stands up to any regulation.

MineOS

Power your data governance. Increase trust.

Learn more here

Follow us on Linkedin