

U.S. STATE CONSUMER PRIVACY LAWS

A Visual Guide with Whiteboards

By Daniel J. Solove

July 2026 Edition

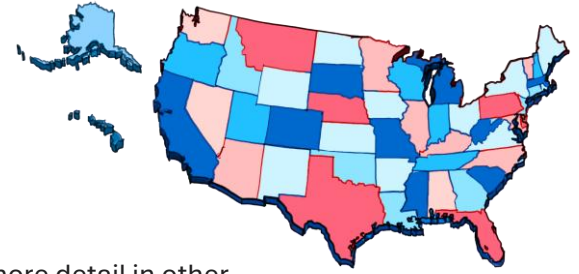


Understanding the Patchwork

Starting in 2018, U.S. states began to enact broad consumer privacy laws. California was the first with the California Consumer Privacy Act (CCPA). By 2026, nearly half the states had enacted similar laws.

At first, the laws can seem like a daunting patchwork, but I believe there's a way to understand them in an easy-to-understand way. Many are structured similarly and take similar approaches. They have differences, but there are more commonalities than divergences.

The purpose of this guide is to be concise and engaging. You'll find a lot more detail in other resources. This guide is different. I aim to focus on what I think are the most important things to highlight and to keep it simple and fun.



Scope and Applicability

All the laws are **extraterritorial**—they apply to entities beyond state borders that do business in the state or collect data about state residents.

Most laws aim to **exempt small businesses**, and they have revenue and/or resident thresholds. Some laws explicitly exempt small businesses as defined by the U.S. Small Business Administration.

Many laws **exempt non-profits and higher ed**, though there are several that don't.

All the laws **exempt data covered by federal laws** such as HIPAA, FERPA, GLBA, and others.



Basic Approach

Nearly all laws take the **notice-and-choice approach**, allowing entities significant freedom to determine how they want to collect and process data. They must provide notice about their data collection and processing.

Individuals can opt out of certain data collection, use, or transfers.

Many laws require opt in for sensitive data, and a few ban the sale of certain types of data.



Personal Data

All the laws adopt GDPR-style definitions of personal data, recognizing identified and identifiable data.

Most laws **exempt publicly-available data**.



Identified

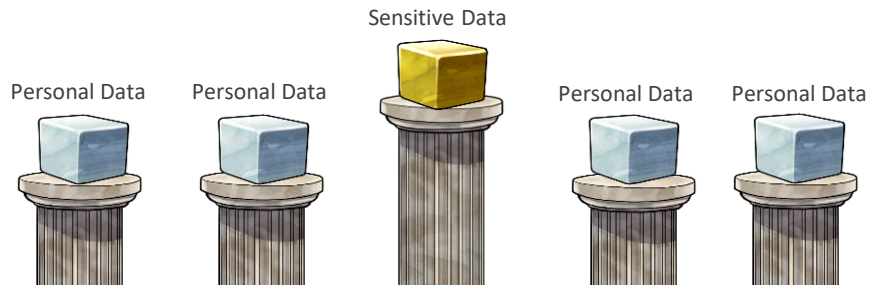


Identifiable

This guide is for personal use only. For distribution, use in presentations, use for institutional training, or use by compliance teams, please contact us at inquiry@teachprivacy.com.

Sensitive Data

All the laws provide **heightened protection for sensitive data**. Most laws require **opt in** and a **privacy impact assessment** to collect or process sensitive data. The laws differ on the categories of data they recognize as sensitive.



Some of the most commonly recognized categories of sensitive data include:

- racial or ethnic origin
- religious beliefs
- sexual orientation and/or sex life
- health condition and/or diagnosis and/or treatment
- data collected from a known child
- precise geolocation
- genetic and biometric data

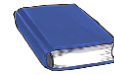
Racial or Ethnic Origin



Sexual Orientation



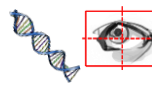
Religious Beliefs



Data Collected from Child



Genetic or Biometric Data



Citizenship or Immigration Status



Mental or Physical Health Diagnosis



Precise Geolocation



Other types of recognized categories include:

- neural data
- transgender or nonbinary status
- government ID information
- financial account information

Neural Data



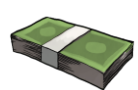
Transgender or Nonbinary Status



Gov't ID Info



Financial Account Info



Individual Rights

Nearly all the laws provide for the following individual rights:

- right to know
- right to access
- right to correct (except Iowa)
- right to delete
- right to data portability

Right to Know



Right to Access



Right to Correction



Right to Deletion



Right to Data Portability



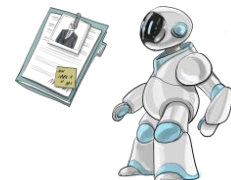
Most laws provide for a right to opt out of certain types of data processing:

- targeted ads
- profiling
- sale of data

Right to Opt Out



A few states provide for **automated profiling decision rights**, such as a right to question the result of profiling, be informed of the reason for a decision, review data used in the decision, and have the decision reevaluated if data was incorrect



Responsibilities for Data Processing

Most laws require the following **responsibilities** for data processing:

- notice
- data minimization (procedural)
- data processing agreements
- reasonable data security
- prohibition on discrimination for exercising rights
- privacy impact assessments
 - targeted ads
 - profiling
 - sensitive data (many states)
 - sale of data

Notice



Data Minimization



Data Security



Privacy Impact Assessments



Data Processing Agreements



Prohibition on Discrimination for Exercising Rights



Some laws have special additional responsibilities and restrictions. A few examples include:

- **Maryland** has a strict **data minimization** requirement, especially for sensitive data.
- Some states have provisions that deem **dark patterns** to be invalid consent.
- Some laws have additional restrictions for **children's data**.

Enforcement

Most laws are enforced by **state attorneys general**. But California has a designated agency to enforce its law.

Most laws have **fines** for violations, which typically range from \$5K to \$10K. Some laws have large fines, including up to \$50K.



Most laws **lack a private right of action**, except California, which has one for data security violations.

Many laws have a **right to cure** (30-60 days). Some sunset but others are permanent.



U.S. State Consumer Privacy Laws Whiteboard

The whiteboard below provides a bird's eye overview of all the state privacy laws.

In the pages that follow, I provide the whiteboards for each state, along with a few key points about each state's law, especially areas where the laws differ.

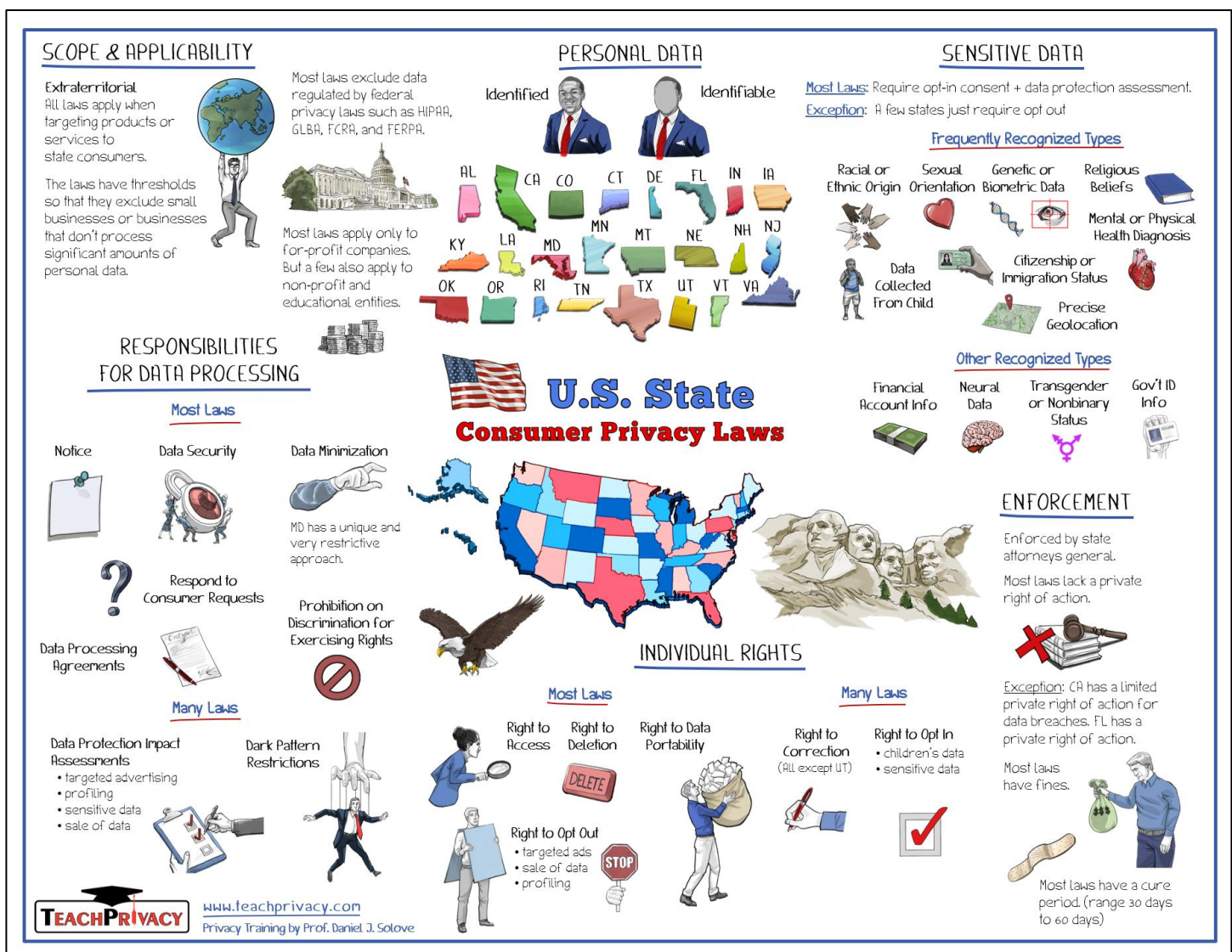
For full-size whiteboards, you can obtain each one individually as a poster or handout.

Some are available free for personal use. Others are only available for a fee. I change up which ones are free, so please stay tuned to my channels to find out when a new one is available.

TeachPrivacy

I created this guide for TeachPrivacy, the privacy training company I founded. For over 15 years, TeachPrivacy has served hundreds of organizations worldwide, providing training on privacy, AI, and data security. We offer 180+ courses and 100+ whiteboards designed to make complex topics accessible and actionable.

If your organization is looking for engaging privacy training, please reach out to us at inquiry@teachprivacy.com.



Staying Connected and Keeping Current

If you're enjoying this guide, I hope you consider subscribing to some of my channels to keep up. I know your time is short and your inbox is cluttered, but I promise to do my best to produce materials you'll want to see.

Newsletter

My **free** weekly newsletter is the best way to keep up with everything I'm writing and doing.

Join about **17,000 subscribers** to find out about my essays, scholarship, whiteboards, cartoons, online webinars, videos, events, and resources like this one.

I'll be **updating this guide** when laws are amended and new laws are enacted, so the newsletter is the best way to find out when new editions are available.

Subscribe to my Newsletter



Substack

I have a Substack newsletter where I post deeper-dive essays. I'm writing on law and policy issues as well as fiction and film about privacy, AI, and tech. It's free.



Subscribe to my Substack

YouTube

Subscribe to my YouTube channel. All my interviews are here, along with video shorts, and some of my speeches and classes.



Subscribe to my YouTube

Privacy Training and Resources

If you like my approach to explaining privacy laws, you might find my privacy training and resources to be useful for your privacy program.

Privacy Training

I have workforce privacy training, along with specialized role-based topics and courses for the privacy team.

I created my training with the belief that privacy expertise matters.

Take your privacy program to the next level. The courses are short, engaging, and very clear.

Catalog of 180+ Courses

Browse the Course Library



Whiteboards

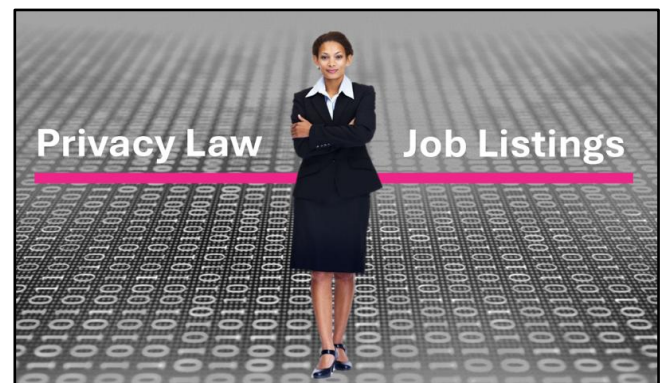
Want full-page versions of the whiteboards or posters? There are whiteboards about federal laws like HIPAA, FERPA, TCPA, and others, as well as whiteboards about privacy laws around the world, including the GDPR.



Browse the Whiteboard Library

Resource Pages

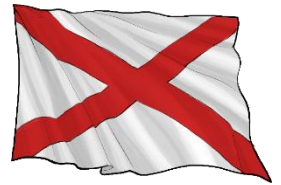
There are countless resource pages on the TeachPrivacy website. For example, I have a page about privacy law job listings which we update every week.



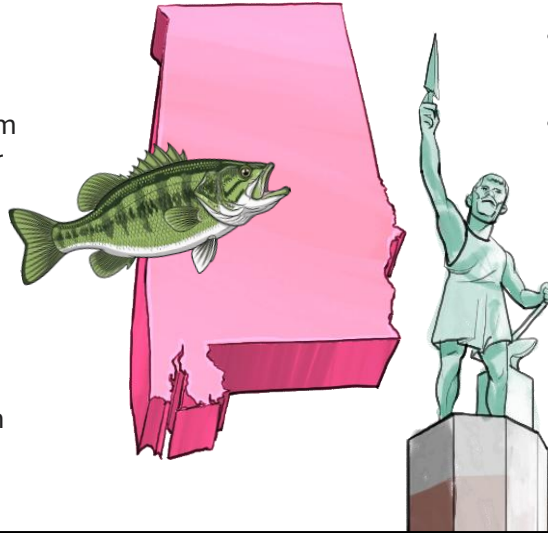
Visit the Job Listings Page

ALABAMA

Personal Data Protection Act



- Enacted in 2026
- Lower threshold than most laws (25K residents or 25% of gross revenue from sale of data with no minimum number of residents)
- Applies to non-profits (but has an exemption for small ones if they don't sell data)
- Permanent cure period
- Fine of \$15,000, which are higher than most states



- Shorter list of sensitive data than other laws
- No requirement for a DPIA for processing sensitive data or for anything else (weaker than most other state laws)



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to AL consumers.



Applies when business controls or process data on
 • at least 25,000 AL residents; or
 • derives 25%+ of gross revenue from sale of data (no min number of residents)

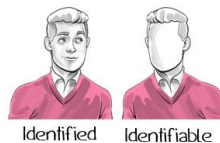
Applies to for-profit companies and non-profits.

Exempts businesses with < 500 employees and non-profits with < 100 employees unless they sell personal data.

Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.



PERSONAL DATA



SENSITIVE PERSONAL DATA

Requires opt-in consent to process. No data protection assessment requirement (unlike most states).



Genetic or Biometric Data



Sexual Orientation



Precise Geolocation



Citizenship or Immigration Status



RESPONSIBILITIES

Notice



Data Quality



Data Minimization



Prohibition on Discrimination for Exercising Rights



Data Security



Data Protection Impact Assessments (DPIA)
No requirement, unlike most states.

Data Processing Agreements



Respond to Consumer Requests
45 days to respond + 45-day extension

ALABAMA
Personal Data Protection Act

INDIVIDUAL RIGHTS

Right to Correct



Right to Delete



Right to Opt Out
• sale of data
• targeted ads
• profiling



Right to Information



Right to Data Portability



ENFORCEMENT

Enforced by the Alabama Attorney General.



No private right of action.



Max fine \$15,000 for violations (higher than most states).

45-day cure period (permanent)



CALIFORNIA

CONSUMER PRIVACY ACT



- Enacted in 2018; amended in 2020; first state consumer privacy law
- Unlike most laws, covers employee data
- Requirement for a button for consumers to click to opt out of selling or sharing of data
- Longer list of sensitive data than other laws; includes neural data, gov't IDs, financial info, union membership, philosophical beliefs, health data
- For significant decisions using automated decision-making technology (ADMT), regulations require human review and special notice to individuals



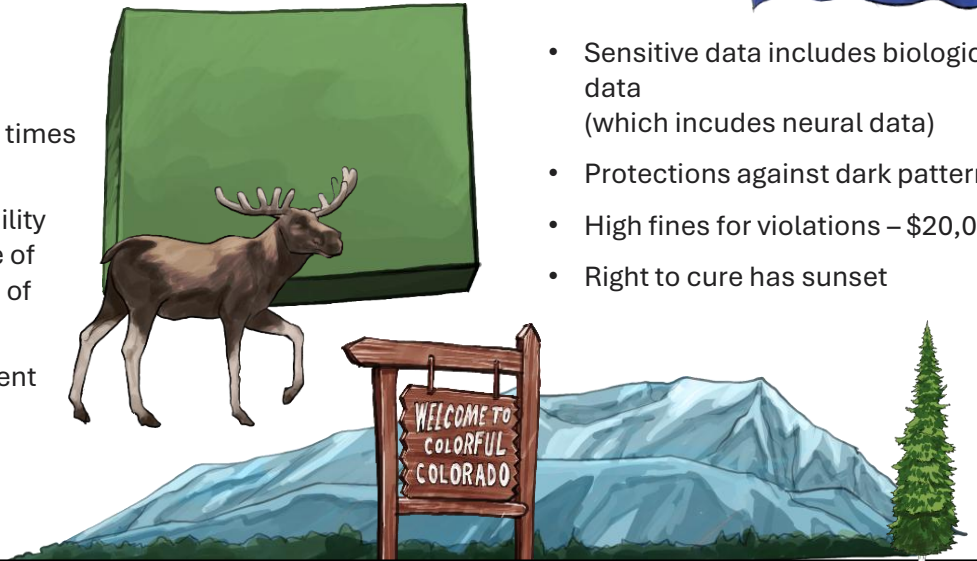
- Opt out rather than opt in to process sensitive data (weaker than most other state laws)
- Dark patterns don't constitute valid consent
- Independent enforcement agency – the California Privacy Protection Agency (CPPA)
- Unlike most laws, has a private right of action (but for data breaches only)
- Unlike most laws, requires training



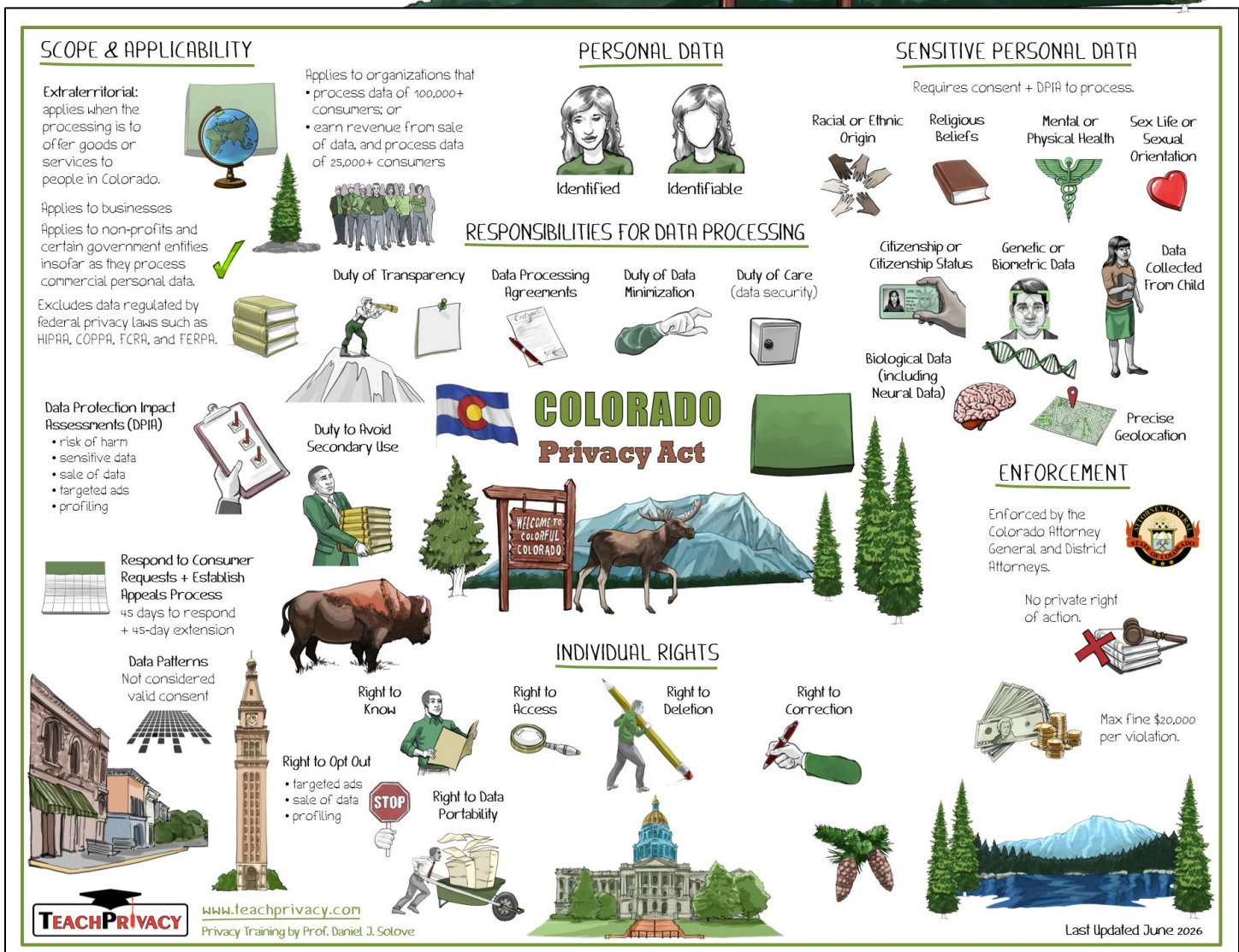
COLORADO Privacy Act



- Enacted in 2021
- Rulemaking authority
- Amended and strengthened several times in 2024-2025
- No general revenue-based applicability threshold. Applies based on volume of data and deriving revenue from sale of data
- Applies to non-profits and government entities if they process commercial personal data



- Sensitive data includes biological data (which includes neural data)
- Protections against dark patterns
- High fines for violations – \$20,000
- Right to cure has sunset

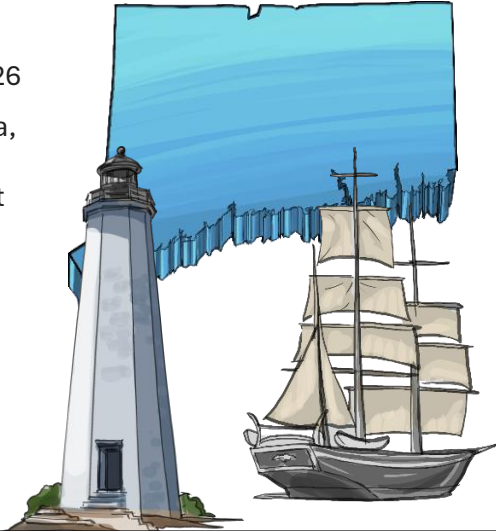


Connecticut

Act Concerning Personal Data Privacy and Online Monitoring



- Enacted in 2022
- Amended and strengthened in 2025-2026
- Recognizes many types of sensitive data, including neural data, transgender or nonbinary status, disability or treatment data, government ID info, and financial account info
- Sensitive data requires consent to sell
- Processing of sensitive data must be "reasonably necessary" for the stated purpose



- Fines up to \$5,000
- Provides for rights regarding automated processing (question outcome, be informed of reasoning, request re-evaluation)
- Right to cure has sunset

SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to CT consumers.



Applies to for-profit companies.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.



Applies when business

- controls or processes personal data on at least 35,000 CT consumers; or
- controls or processes sensitive data (no threshold); or
- offers personal data for sale (no threshold)

Data Protection Impact Assessments (DPIA)

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Prohibition on Discrimination for Exercising Rights



Data Minimization



Respond to Consumer Requests
45 days to respond
+ 45-day extension



Right to Opt Out
• targeted ads
• sale of data
• profiling



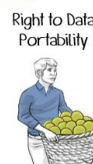
Right to Access



Right to Deletion



Right to Correction



Right to Data Portability



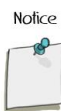
INDIVIDUAL RIGHTS

PERSONAL DATA



Identified Identifiable

RESPONSIBILITIES FOR DATA PROCESSING



Notice



Data Processing Agreements



Data Security

SENSITIVE DATA

Requires consent + DPIA to process. + must be "reasonably necessary" for stated purpose
Requires consent to sell

Racial or Ethnic Origin



Data Collected From Child



Religious Beliefs



Mental or Physical Health Diagnosis



Neural Data



Sexual Orientation



Precise Geolocation



Transgender or Nonbinary Status



Disability or Treatment Data



Citizenship or Immigration Status



Gov't ID Info



Financial Account Info



ENFORCEMENT

Enforced by the CT Attorney General



No private right of action.



Max fine \$5,000 per violation

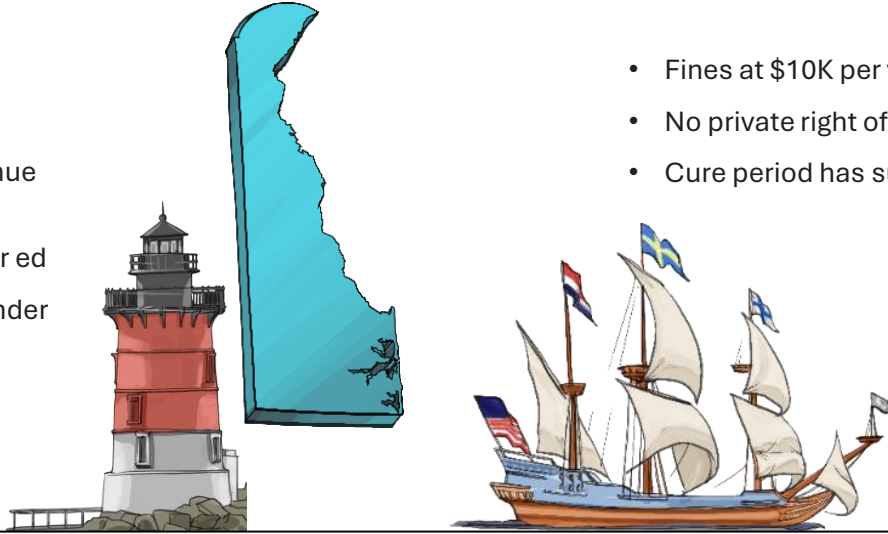
DELAWARE

Personal Data Privacy Act



- Enacted in 2023
- Fairly standard law of its type
- Has low business size and revenue percentage thresholds
- Applies to non-profits and higher ed
- Sensitive data includes transgender or non-binary status

- Fines at \$10K per violation
- No private right of action
- Cure period has sunset



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to DE consumers.



Applies when business controls or process data on

- at least 35,000 DE residents; or
- at least 10,000 DE residents and derives 20%+ of gross revenue from sale of data



Data Protection Impact Assessments

- risk of harm
- sale of data
- targeted ads
- profiling
- sensitive data

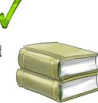
Respond to Consumer Requests and Appeals Process
45 days to respond
+ 45-day extension



Applies to for-profit companies.



Applies to non-profits and higher ed.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.

PERSONAL DATA

Identified



Identifiable

SENSITIVE PERSONAL DATA

Requires consent + DPIA (risk of unfair or deceptive treatment or unlawful disparate impact).

Racial or Ethnic Origin



Data of Known Child



Religious Beliefs



Genetic or Biometric Data



Mental or Physical Health Condition or Diagnosis



Sexual Orientation



Sex Life



Precise Geolocation



Status as Transgender or Non-Binary



Citizenship or Immigration Status



RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing Agreements



Data Minimization



Data Security



DELAWARE

Personal Data Privacy Act



ENFORCEMENT

Enforced by the Delaware Attorney General.



INDIVIDUAL RIGHTS

Right to Know



Right to Access



Right to Correction



Right to Deletion



Right to Data Portability



Right to Opt Out

- targeted ads
- sale of data
- profiling for solely automated decisions



No private right of action.

Max fine \$10,000

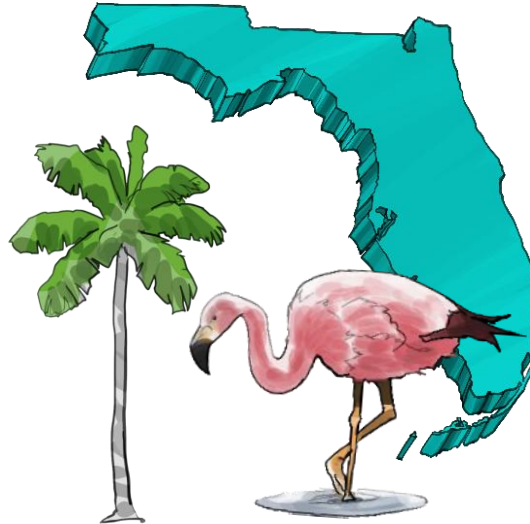


Florida

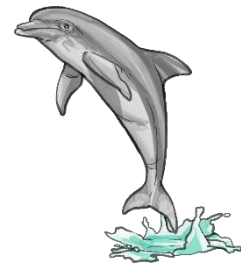
Digital Bill of Rights



- Enacted in 2023
- Very high thresholds for applicability—\$1B+ in revenue and other requirements
- Targeted mainly to the largest platforms and search engines
- Short list of sensitive data
- Search engines must disclose factors in search rankings, including the role of politics



- Very high fines at \$50K per violation, which can be trebled
- No private right of action
- Cure period doesn't sunset



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to FL consumers.

Applies to for-profit companies.

Excludes non-profits and higher ed.

Excludes data regulated by federal privacy laws such as HIPAA, FCRA, FERPA, GLBA, or COPPA.

Applies when:

- ▶ business collects and controls the purposes of processing personal data; and
- ▶ \$1 billion+ in global revenue; and
- ▶ one of the following:
 - at least 50% of gross revenue from sale of ads online
 - operates a hands-free speaker/voice virtual assistant service (excluding autos)
 - operates app store or digital platform with at least 250,000 different software apps

PERSONAL DATA

Identified Identifiable

RESPONSIBILITIES FOR DATA PROCESSING

Notice Data Processing Agreements Data Security

Prohibition on Discrimination for Exercising Rights Data Minimization

Data Protection Impact Assessments (DPIA)

SENSITIVE DATA

Processing of sensitive data requires prior consent.

Racial or Ethnic Origin

Mental or Physical Health Diagnosis

Religious Beliefs

Precise Geolocation

Genetic or Biometric Data

Sexual Orientation

Citizenship or Immigration Status

Data Collected From Child

SPECIAL PROTECTIONS

Search Engine Disclosures
Disclose most significant factors in search result rankings including role of politics in the ranking.

Protection of Children Online
Prohibits practices posing substantial harm or privacy risk to children.

Government Content Moderation
Prohibits gov't from requesting content moderation.

Respond to Consumer Requests
45 days to respond + 15-day extension

INDIVIDUAL RIGHTS

Right to Know Right to Access Right to Delete Right to Data Portability Right to Correct

Right to Opt Out

- sale of data
- targeted ads
- sensitive data
- collection of data through voice or facial recognition features

ENFORCEMENT

Enforced by the FL Attorney General.

No private right of action.

Max fine \$50,000 per violation.

45-day cure period

Fines trebled if involving a known child, failing to delete or correct consumer data after receiving authenticated request, or continuing to sell or share data after opt out.

Florida Digital Bill of Rights

TEACHPRIVACY

www.teachprivacy.com

Privacy Training by Prof. Daniel J. Solove

Last Updated June 2026

INDIANA

Consumer Data Protection Act



- Enacted in 2023
- Fairly standard law of its type
- No notable outlier provisions
- Fines at \$7.5K per violation
- No private right of action
- Permanent cure period



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to IN consumers.



Applies when business controls or process data on

- at least 100K IN consumers; or
- at least 25K IN consumers + 25% of gross revenue

Data Protection Impact Assessments

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Respond to Consumer Requests
45 days to respond + 45-day extension

Applies to for-profit companies.



Excludes non-profits and higher ed.
Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.

Prohibition on Discrimination for Exercising Rights



Data Minimization



PERSONAL DATA

Identified



Identifiable

RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing Agreements



Data Security



Racial or Ethnic Origin



Requires consent + DPIA to process.

Data Collected From Known Child



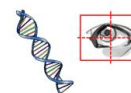
Religious Beliefs



Mental or Physical Health Diagnosis



Genetic or Biometric Data



Precise Geolocation



Sexual Orientation



Citizenship or Immigration Status



ENFORCEMENT

Enforced by the Indiana Attorney General.



No private right of action.



Max fine \$7,500 per violation



30-day cure period (permanent).



INDIVIDUAL RIGHTS

Right to Know



Right to Access



Right to Delete



Right to Correction



Right to Data Portability



Right to Opt Out

- targeted ads
- sale of data
- profiling



IOWA

Consumer Data Protection Act



- Enacted in 2023
- One of the weakest state privacy laws
- Fairly high applicability thresholds for a state its size
- Lacks opt out of target ads
- Opt out rather than opt in for processing sensitive data
- Only has opt out for sale of data. Unlike most other laws, doesn't include the right to opt out of targeted ads or profiling

- Lacks a right to correction
- No DPIA requirement
- Fines at \$7.5K per violation
- No private right of action
- Cure period is 90 days, the longest of all the laws, and it doesn't sunset

SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to IA consumers.



Applies when business controls or process data on

- at least 100,000 IA consumers; or
- at least 50% of gross revenue from processing data on at least 25,000 IA consumers

Data Protection Impact Assessments (DPIA)
Not required

Respond to Consumer Requests
90 days to respond
+ 45-day extension



Applies to for-profit companies.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.
Excludes non-profits and higher ed.



Identified Identifiable



Excludes publicly-available data.

PERSONAL DATA

RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing Agreements



Data Security



Racial or Ethnic Origin



Mental or Physical Health Diagnosis



Religious Beliefs



Precise Geolocation



Genetic or Biometric Data



Sexual Orientation



Citizenship or Immigration Status



Data Collected From Child



Default opt in for children's data

Prohibition on Discrimination for Exercising Rights



IOWA Consumer Data Protection Act



INDIVIDUAL RIGHTS

Right to Know



Right to Access



Right to Delete



Right to Data Portability



Right to Correction
Not included

Right to Opt Out
• sale of data only

Unlike many other laws, doesn't include right to opt out of targeted ads or profiling



ENFORCEMENT

Enforced by the IA Attorney General.



No private right of action.



Max fine \$7,500 per violation



90-day cure period (permanent)



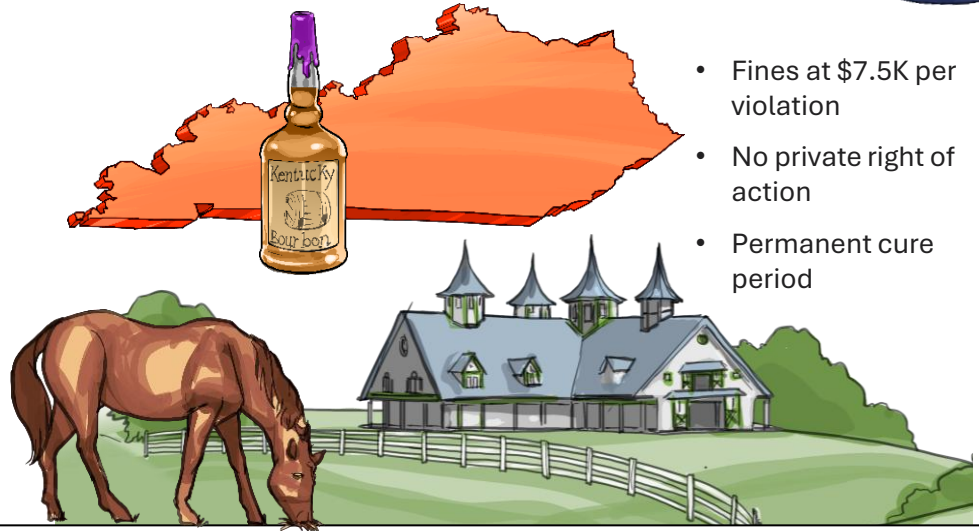
Last Updated June 2026

KENTUCKY

Consumer Data Protection Act



- Enacted in 2024
- Fairly standard law of its type
- Few notable outlier provisions
- Recognizes “automated content recognition data” as sensitive data. This data involves “data about a consumer’s content viewing history collected through the use of technology that is embedded or operated through a smart television or smart monitor.”



- Fines at \$7.5K per violation
- No private right of action
- Permanent cure period

SCOPE & APPLICABILITY

Extraterritorial

Applies when targeting products or services to KY consumers.



Applies when entities control or process data on:

- at least 100K KY consumers; or
- at least 25K KY consumers and derives at least 50% of gross revenue from sale of data



Data Protection Impact Assessments (DPIA)

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Respond to Consumer Requests and Appeals Process

45 days to respond + 45-day extension



Applies to for-profit companies.

Excludes non-profits and higher education.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, and FCRA.



Data Processing Agreements



Prohibition on Discrimination for Exercising Rights



PERSONAL DATA

Identified

Identifiable



RESPONSIBILITIES FOR DATA PROCESSING

Notice

Data Minimization

Data Security



SENSITIVE PERSONAL DATA

Requires consent + DPIA to process + prohibition on sale.

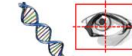
Racial or Ethnic Origin



Mental or Physical Health Diagnosis



Genetic or Biometric Data



Sexual Orientation



Religious Beliefs



Precise Geolocation



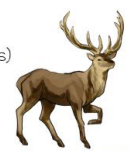
Data Collected From Known Minor



Citizenship or Immigration Status



Automated Content Recognition Data (smart TVs and monitors)



KENTUCKY Consumer Data Protection Act



INDIVIDUAL RIGHTS

Right to Confirm (Know)



Right to Access



Right to Deletion



Right to Correction

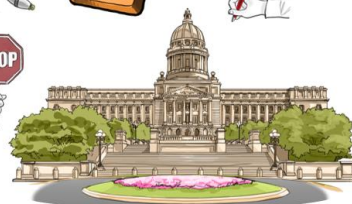


Right to Data Portability



Right to Opt Out

- targeted ads
- sale of data
- profiling



ENFORCEMENT

Enforced by the KY Attorney General.



No private right of action.



Max fine \$7,500.

30-day cure period (does not sunset).



Last Updated June 2026

LOUISIANA

Data Privacy Act



- Enacted in 2026
- Fairly standard law of its type
- Short list of sensitive data
- On the thinner side of most state consumer privacy laws

- Fines at \$5K per violation
- No private right of action
- Cure period has sunset



SCOPE & APPLICABILITY

Extraterritorial
Applies when doing business in LA.



Applies to
for-profit
companies.



Excludes non-profits
and higher education.



Excludes data regulated by
federal privacy laws such as
HIPAA, GLBA, and FCRA.



Applies when business

- has gross revenue of \$25M+ or
- buys, receives, sells, or shares data on 75K+ consumers, or
- derives 50% of annual revenue from data sale

RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing
Agreements



Prohibition on
Discrimination for
Exercising Rights



Data Security



Data Protection Impact
Assessments (DPIA)

- targeted advertising
- profiling
- sale of data
- sensitive data
- heightened risk of harm



Respond to
Consumer Requests
45 days to respond
+ 45-day extension



Data
Minimization



Right to
Know



- Right to Opt Out
- targeted advertising
- sale of data
- profiling



Right to
Deletion



Right to
Correction



Right to
Access



Right to Data
Portability

LOUISIANA
Data Privacy Act

SENSITIVE DATA

Requires consent + DPIA to process.

Racial or
Ethnic Origin



Genetic or
Biometric Data



Data Collected
from Known
Child



Precise
Geolocation



Sexuality



Religious
Beliefs



Mental or Physical
Health Diagnosis



Citizenship or
Immigration Status



ENFORCEMENT

Enforced by the LA
Attorney General.



No private right
of action.



\$5,000 fine
for violations

30-day cure period.
Sunsets July 31, 2027

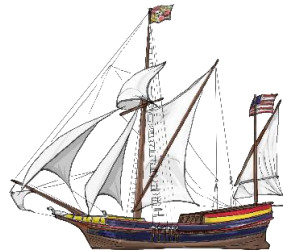
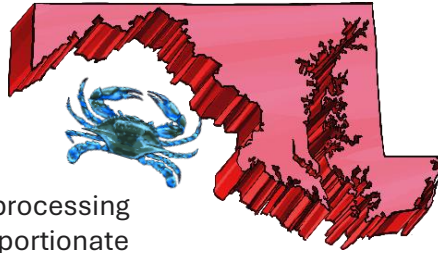


MARYLAND

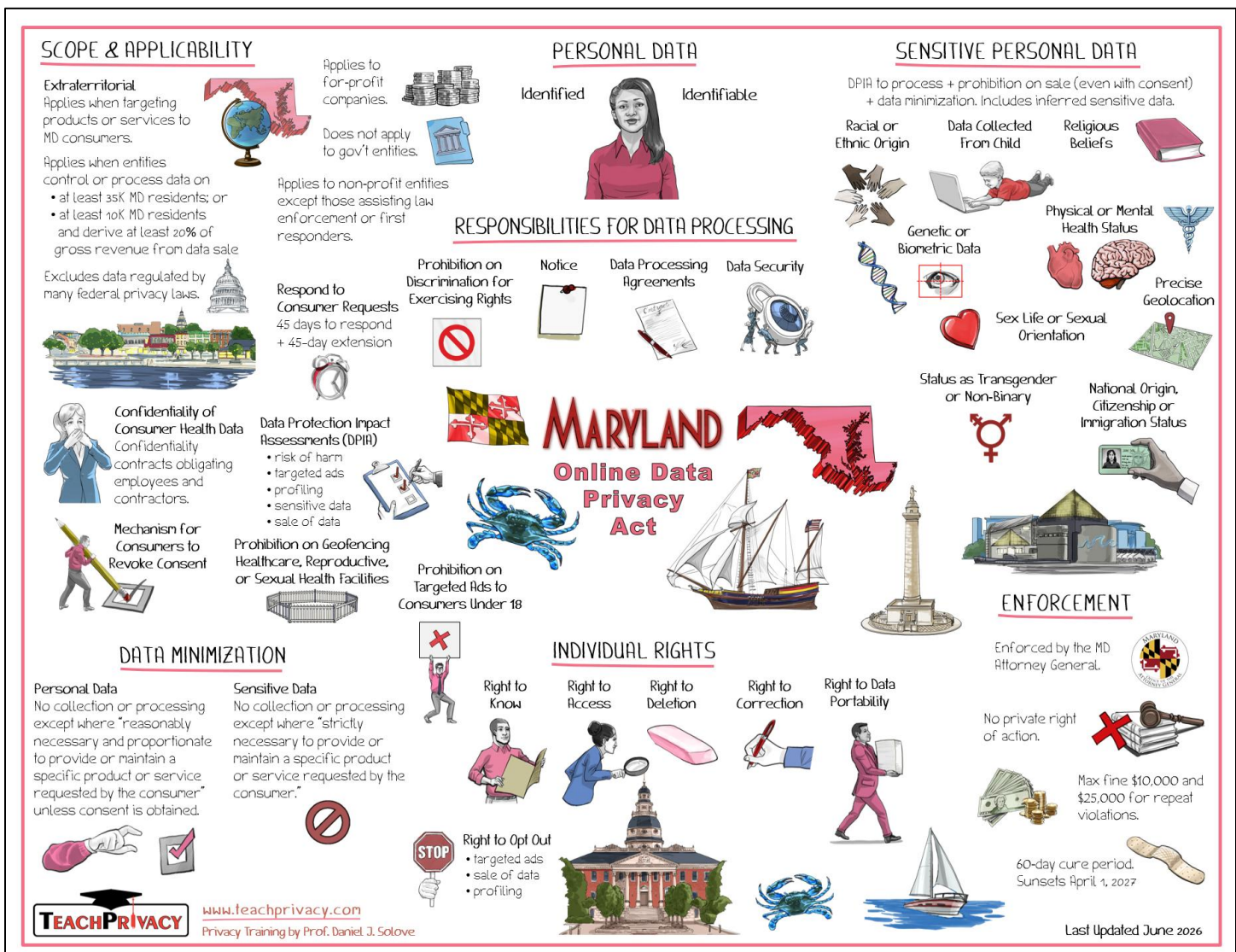
Online Data Privacy Act



- Enacted in 2024
- Has the strongest data minimization requirements of any state consumer privacy law
- Data minimization for personal data—processing must be reasonably necessary and proportionate to provide the product or service requested (unless consent is obtained)
- Data minimization for sensitive data—processing must be strictly necessary to provide product or service requested. No consent exception.
- Consumers can revoke consent



- Applies to non-profits
- Geofencing restrictions
- Sensitive data includes inferred sensitive data
- Sensitive data includes transgender or non-binary status
- Fines at \$10K per violation, \$25K for repeat violations
- No private right of action
- Cure period, but will sunset on April 1, 2027

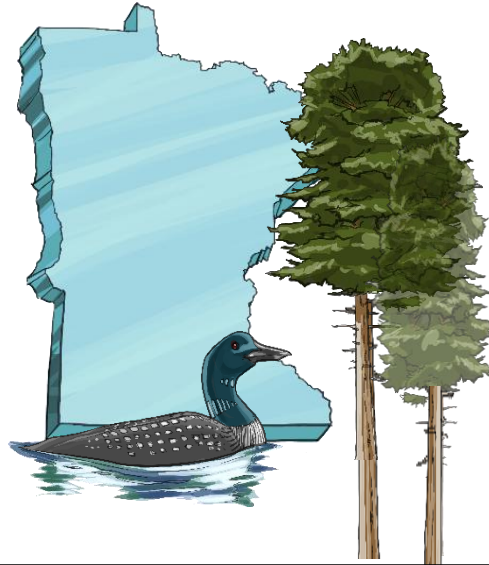


minnesota

Consumer Data Protection Act



- Enacted in 2024
- Fairly standard law of its type
- Standard list of sensitive data
- Applies to non-profits
- One of only a few state to exempt small businesses (as defined by the Small Business Administration). But still requires small business to obtain consumer consent before selling sensitive data



- One of a few states to provide for profiling rights, such as a right to question the result of profiling, be informed of the reason for a decision, review data used in the decision, have the decision reevaluated if data was incorrect
- Fines at \$5K per violation
- No private right of action
- Cure period has sunset

SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to Minnesota consumers.



The CDPA applies when entities control or process data on

- at least 100K MN residents; or
- at least 25K MN residents and derives at least 25% of gross revenue from sale of data

Excludes small businesses as defined by U.S. Small Business Administration.



Data Protection Impact Assessments (DPIA)

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Prohibition on Discrimination for Exercising Rights



Respond to Consumer Requests and Appeals Process
45 days to respond
+ 45-day extension



Right to Know



Right to Opt Out

- targeted ads
- sale of data
- profiling



Right to Access



Right to Deletion



Right to Data Portability



Right to Correction



Question Results of Profiling



No private right of action.



Max fine \$7,500.



SENSITIVE PERSONAL DATA

Requires consent + DPIA to process.

Racial or Ethnic Origin



Data Collected From Child



Religious Beliefs



Mental or Physical Health Diagnosis



Genetic or Biometric Data



Sexual Orientation



Citizenship or Immigration Status



Specific Geolocation



PERSONAL DATA



Identified Identifiable

RESPONSIBILITIES FOR DATA PROCESSING

Data Processing Agreements



Data Minimization



Data Security



minnesota Consumer Data Protection Act



ENFORCEMENT

Enforced by the MN Attorney General.

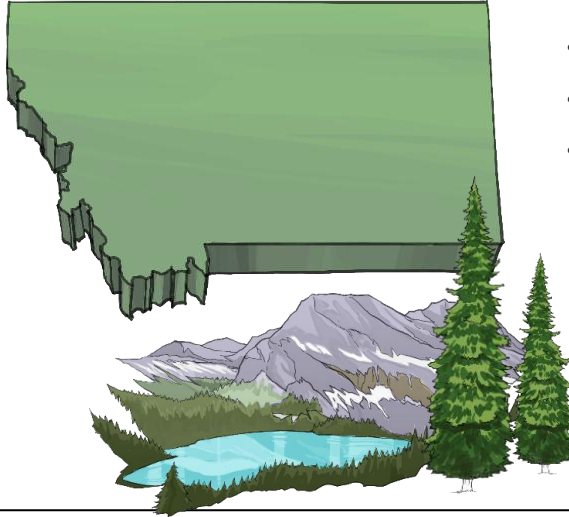


Montana

Consumer Data Privacy Act



- Enacted in 2023
- Amended in 2025
- Applicability threshold doesn't apply when data of minors (under 18) is involved
- Covers most non-profits
- Fairly standard law of its type
- Standard list of sensitive data

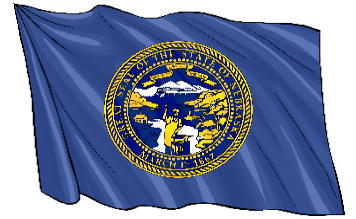


- Fines at \$7.5K per violation
- No private right of action
- Right to cure eliminated in an amendment



NEBRASKA

Data Privacy Act



- Enacted in 2024
- Fairly standard law of its type
- Only one of a few laws to lack size or revenue applicability thresholds; instead, it exempts small businesses (as determined by the federal Small Business Act)
- Standard list of sensitive data



- Fines at \$7.5K per violation
- No private right of action
- Cure period is permanent

SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to NE consumers.



Lacks thresholds for number of consumers and revenue but exempts small businesses (as determined by the federal Small Business Act).

Data Protection Impact Assessments (DPIA)

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Respond to Consumer Requests
45 days to respond
+ 45-day extension



Applies to for-profit companies.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.
Excludes non-profits and higher ed.



PERSONAL DATA

Identified
Identifiable



Excludes publicly-available data.

RESPONSIBILITIES FOR DATA PROCESSING



Notice

Data Processing Agreements



Data Security



SENSITIVE DATA

Requires opt in + DPIA to process sensitive data.

Racial or Ethnic Origin



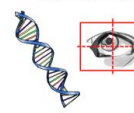
Mental or Physical Health Diagnosis



Religious Beliefs



Genetic or Biometric Data



Sexual Orientation



Citizenship or Immigration Status



Data Collected From Child



Precise Geolocation



NEBRASKA Data Privacy Act



ENFORCEMENT

Enforced by the NE Attorney General.



No private right of action.



Max fine \$7,500 per violation



30-day cure period (permanent)



INDIVIDUAL RIGHTS

Right to Know



Right to Access



Right to Delete



Right to Correction



Right to Data Portability



Right to Opt Out
• sale of data
• targeted ads
• profiling



NEW HAMPSHIRE

PRIVACY ACT



- Enacted in 2024
- Fairly standard law of its type
- Standard list of sensitive data
- Amended in 2026 to prohibit the sale of children's data

- Fines at \$10K per violation
- No private right of action
- Cure period is discretionary



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to NH consumers.



Applies when business controls or process data on

- at least 35,000 NH residents (excluding payment transactions); or
- 10,000 residents + 25% revenue from personal data sale



Data Protection Impact Assessments (DPIA)

- targeted advertising
- profiling
- sale of data
- sensitive data
- heightened risk of harm



Respond to Consumer Requests
45 days to respond
+ 45-day extension



Applies to for-profit companies.



Excludes non-profits and higher education.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, and FCRA.



Prohibition on Discrimination for Exercising Rights



Data Minimization



Right to Know



Right to Access



Right to Opt Out

- targeted advertising
- sale of data
- profiling



PERSONAL DATA

Identified



Identifiable

RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing Agreements



Data Security



SENSITIVE DATA

Requires consent + DPIA to process.
Prohibits sale of children's data.



Racial or Ethnic Origin



Known Child (under 13) Personal Data



Religious Beliefs



Mental or Physical Health Condition or Diagnosis



Genetic or Biometric Data



Precise Geolocation



Sex Life or Sexual Orientation



Citizenship or Immigration Status



ENFORCEMENT

Enforced by the NH Attorney General.



No private right of action.



Fines up to \$10,000.



60-day cure period (discretionary)



INDIVIDUAL RIGHTS

Right to Deletion



Right to Correction

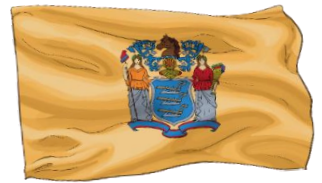


Right to Data Portability



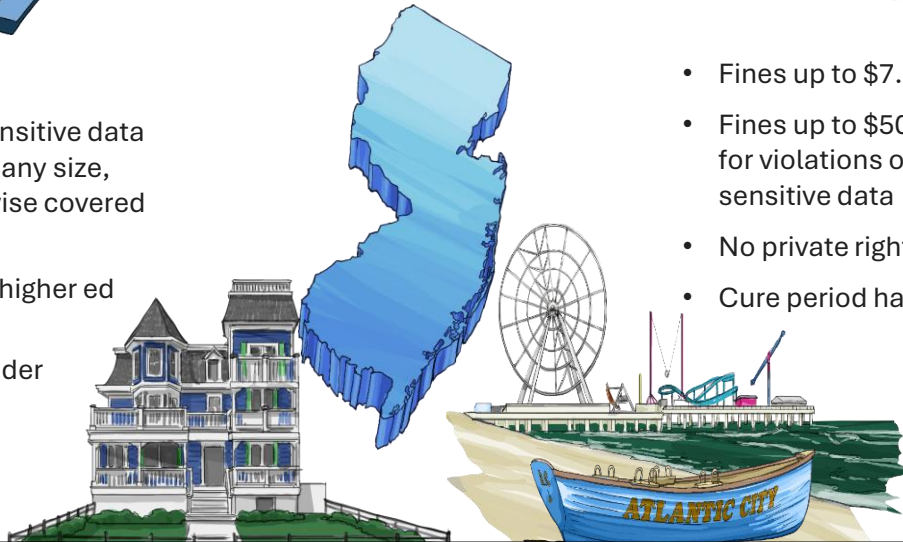


Data Privacy Act



- Enacted in 2024
- Amended to ban sale of sensitive data (applies even to entities of any size, including those not otherwise covered by the Act)
- Applies to non-profits and higher ed
- Sensitive data includes financial info and transgender or non-binary status
- Protects children from targeted ads

- Fines up to \$7.5K per violation
- Fines up to \$50,000 per record for violations of ban on sales of sensitive data
- No private right of action
- Cure period has sunset



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to NJ consumers.



Applies when business controls or process data on

- at least 100,000 NJ consumers; or
- at least 25,000 NJ consumers + derive revenue from sale of personal data

Applies to for-profit companies.



Covers non-profits and higher ed.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, and FCRA. Doesn't exclude FERPA data.



Data Protection Impact Assessments (DPIA)

- targeted advertising
- profiling
- sale of data
- sensitive data
- heightened risk of harm



Respond to Consumer Requests
45 days to respond + 45-day extension



Prohibition on Discrimination for Exercising Rights



Data Minimization



Right to Know



Right to Access



Right to Opt Out

- targeted advertising
- sale of data
- profiling



PERSONAL DATA

Identified

Identifiable



RESPONSIBILITIES FOR DATA PROCESSING

Notice



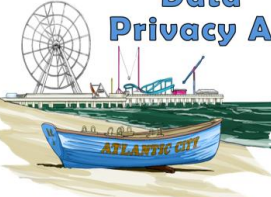
Data Processing Agreements



Data Security



Data Privacy Act



SENSITIVE DATA

Requires consent + DPIA to process.

Ban on sale of sensitive data (even if not otherwise covered by the NJ Privacy Act)



Racial or Ethnic Origin



Child's Personal Data



Religious Beliefs



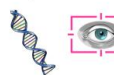
Financial Info (includes account info)



Mental or Physical Condition, Treatment, or Diagnosis



Genetic or Biometric Data



Precise Geolocation



Status as Transgender or Nonbinary



Sex Life or Sexual Orientation



Citizenship or Immigration Status



ENFORCEMENT

Enforced by the New Jersey Attorney General.



No private right of action.



Fines up to \$7,500

Fines up to \$50,000 per record for violating ban on sale of sensitive data

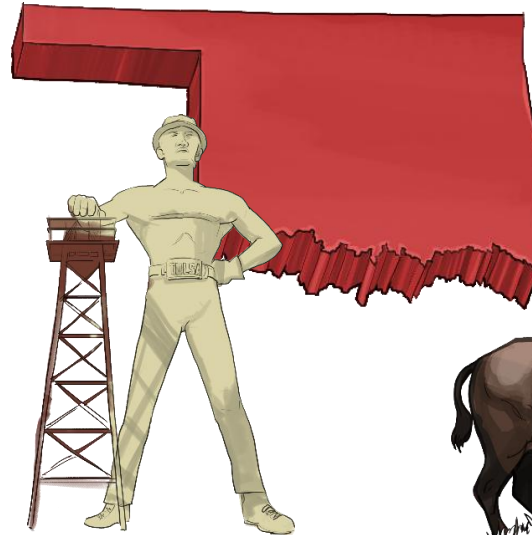
Last Updated July 2026

OKLAHOMA

Data Privacy Act



- Enacted in 2026
- Fairly standard law of its type
- Short list of sensitive data
- On the thinner side of most state consumer privacy laws



- Fines at \$7.5K per violation
- No private right of action
- Cure period is permanent

SCOPE & APPLICABILITY

Extraterritorial
Applies doing business in OK or targeting products or services to OK residents.

Applies when business

- controls or processes data on 100,000+ consumers; or
- controls or processes data on 25,000+ consumers and derives 50%+ of annual revenue from personal data sale

PERSONAL DATA

Identified **Identifiable**

Excludes non-profits and higher education.

Excludes data regulated by federal privacy laws such as HIPAA, GLBA, and FCRA.

SENSITIVE DATA

Requires consent + DPIA to process.

- Racial or Ethnic Origin
- Data Collected from Known Child
- Religious Beliefs
- Mental or Physical Health Diagnosis
- Genetic or Biometric Data
- Sexual Orientation
- Precise Geolocation
- Citizenship or Immigration Status

OKLAHOMA Data Privacy Act

RESPONSIBILITIES FOR DATA PROCESSING

- Notice**
- Data Processing Agreements**
- Prohibition on Discrimination for Exercising Rights**
- Data Protection Impact Assessments (DPIA)**
 - targeted advertising
 - profiling
 - sale of data
 - sensitive data
 - heightened risk of harm
- Data Security**
- Data Minimization**
- Respond to Consumer Requests**
45 days to respond + 45-day extension

INDIVIDUAL RIGHTS

- Right to Know**
- Right to Deletion**
- Right to Correction**
- Right to Data Portability**
- Right to Opt Out**
 - targeted advertising
 - sale of data
 - profiling
- Right to Access**

ENFORCEMENT

Enforced by the OK Attorney General.

No private right of action.

Max fine \$7,500 per violation.

30-day cure period (permanent).

OKLAHOMA Data Privacy Act

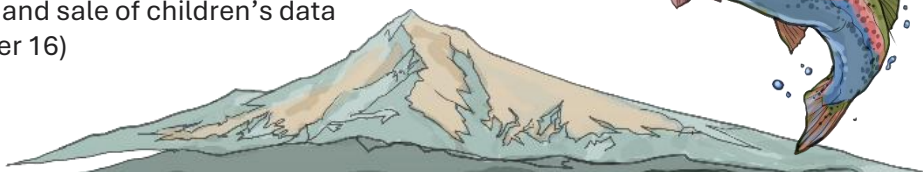
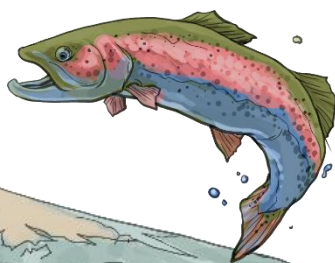
www.teachprivacy.com
 Privacy Training by Prof. Daniel J. Solove

Oregon

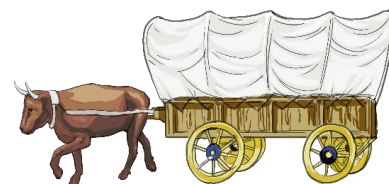
Consumer Privacy Act



- Enacted in 2023
- Amended in 2025
- Applies to non-profits
- Sensitive data includes transgender or non-binary status and crime victim status
- Ban on sale of precise geolocation data and sale of children's data (under 16)



- Dark patterns not considered valid consent
- Fines up to \$7.5K per violation
- No private right of action
- Cure period has sunset



SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to OR consumers.



Applies when business controls or process data on

- at least 100,000 OR consumers; or
- at least 25,000 OR consumers + 25% of gross revenue



Data Protection Impact Assessments (DPIA)

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Respond to Consumer Requests
45 days to respond
+ 45-day extension



Data Patterns
Not considered valid consent

Right to Know

Right to Deletion

Right to Correction

Right to Data Portability

Right to Opt Out

- targeted advertising
- sale of data
- profiling



Applies to for-profit companies.



Covers non-profits except those to detect insurance fraud and radio/TV networks.

Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.



PERSONAL DATA

Identified



Identifiable

RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing Agreements



Data Security



SENSITIVE DATA

Requires opt-in + DPIA to process.

Ban on sale of precise geolocation data and sale of children's data (under 16)



Racial or Ethnic Origin



Child's Personal Data



Religious Beliefs

Mental or Physical Condition or Diagnosis



Genetic or Biometric Data



Precise Geolocation



Transgender or Nonbinary Status



Sexual Orientation



Citizenship or Immigration Status



Crime Victim Status



ENFORCEMENT

Enforced by the Oregon Attorney General.



No private right of action.



Max Fine
\$7,500



INDIVIDUAL RIGHTS

Right to Know

Right to Deletion

Right to Correction

Right to Data Portability

Right to Opt Out

- targeted advertising
- sale of data
- profiling

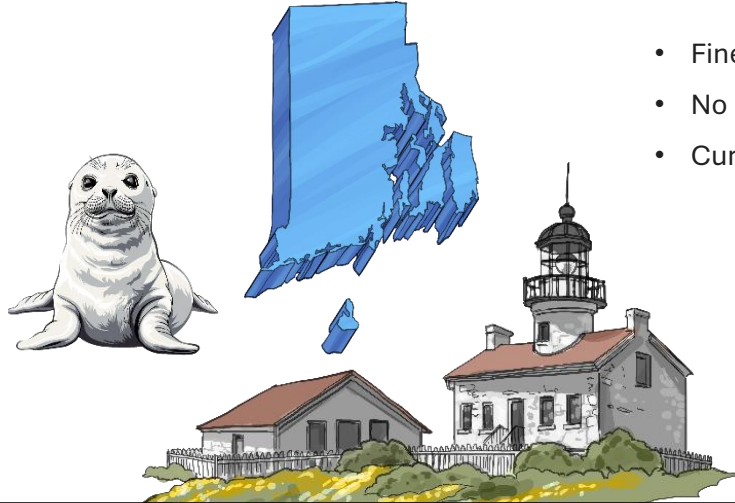


RHODE ISLAND

Data Transparency and Privacy Protection Act



- Enacted in 2024
- Fairly standard law of its type
- Standard list of sensitive data
- Lacks data minimization restrictions



- Fines at \$10K per violation
- No private right of action
- Cure period has sunset

SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to RI consumers.



Applies to for-profit companies.

Does not apply to non-profit entities, gov't, or higher ed.

Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.



PERSONAL DATA

Identified

Identifiable



SENSITIVE PERSONAL DATA

Requires consent + DPIA to process.



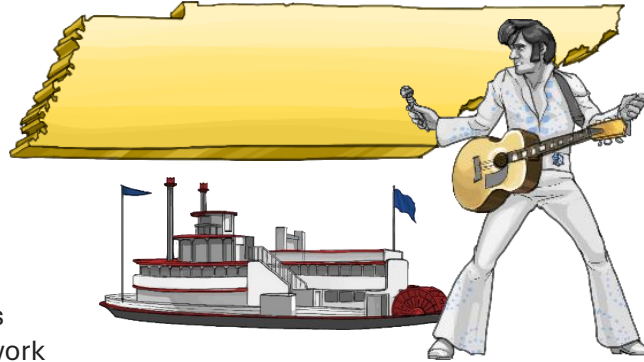
Racial or Ethnic Origin

Data Collected From Child

Religious Beliefs

Tennessee

Information Protection Act



- Enacted in 2023
- High applicability threshold; must have \$25M+ in revenue
- Fairly standard state consumer privacy law
- Standard list of sensitive data
- Affirmative defense if a business follows the NIST Privacy Framework

- Fines at \$7.5K per violation
- No private right of action
- Permanent cure period

SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to IN consumers.



Applies when business controls or process data on

- at least \$25m in revenue; and
- at least 175,000 IN consumers; or
- at least 25,000 IN consumers + 50% of gross revenue

Applies to for-profit companies.



Excludes non-profits and higher ed.
Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.



Data Protection Impact Assessments

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Prohibition on Discrimination for Exercising Rights



Data Minimization



Respond to Consumer Requests
45 days to respond + 45-day extension



PERSONAL DATA

Identified



Identifiable

RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Processing Agreements



Data Security



Tennessee Information Protection Act



SENSITIVE DATA

Requires consent + DPIA to process.

Racial or Ethnic Origin



Data Collected From Known Child



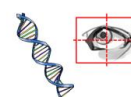
Religious Beliefs



Mental or Physical Health Diagnosis



Genetic or Biometric Data



Precise Geolocation



Sexual Orientation



Citizenship or Immigration Status



ENFORCEMENT

Enforced by the Tennessee Attorney General.



No private right of action.



Max fine \$7,500 per violation

60-day cure period (permanent)



Safe Harbor
Affirmative defense if follows NIST Privacy Framework.



INDIVIDUAL RIGHTS

Right to Know



Right to Access



Right to Delete



Right to Correction



Right to Data Portability

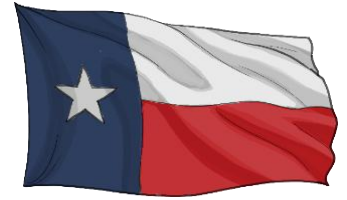


Right to Opt Out
• targeted ads
• sale of data
• profiling



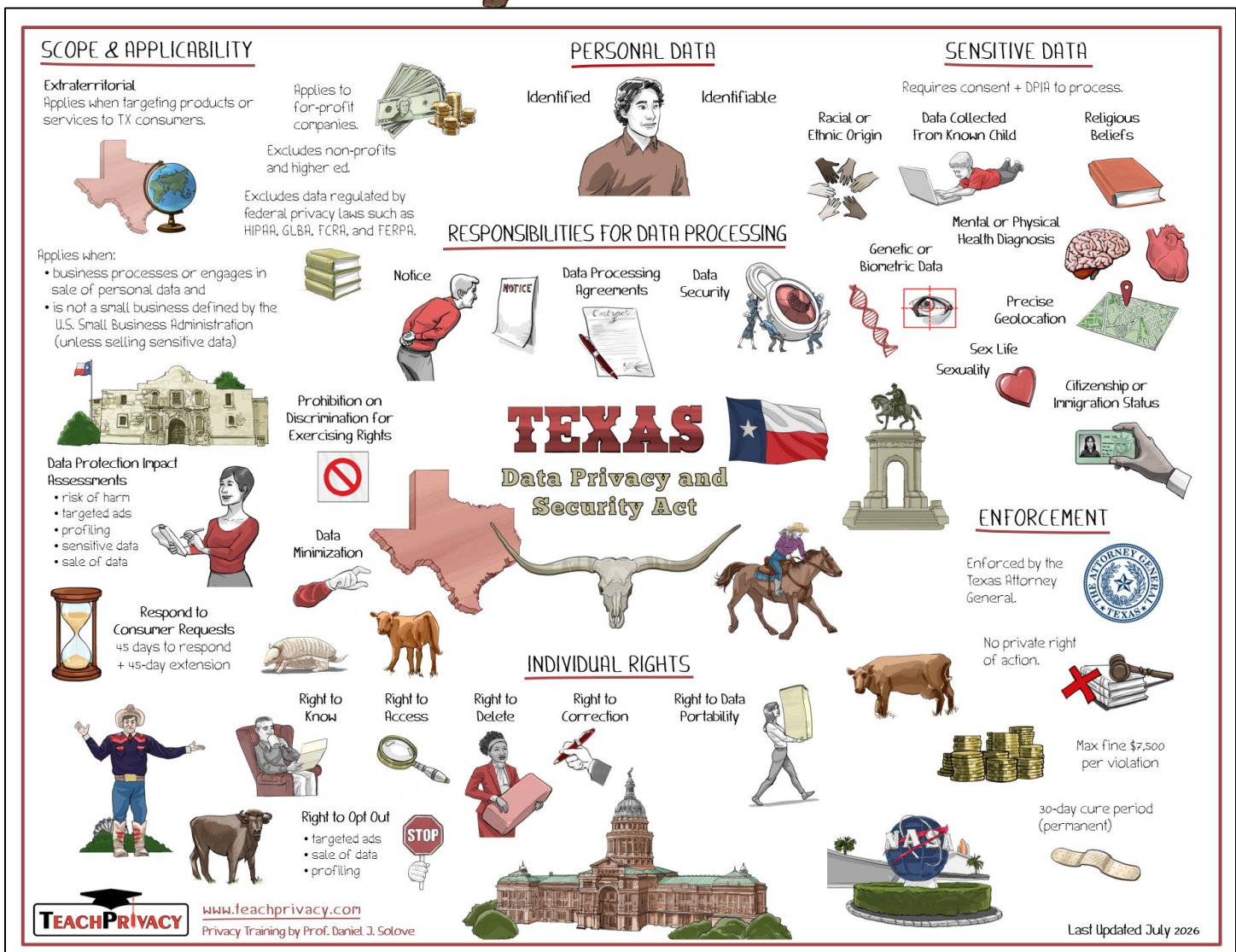
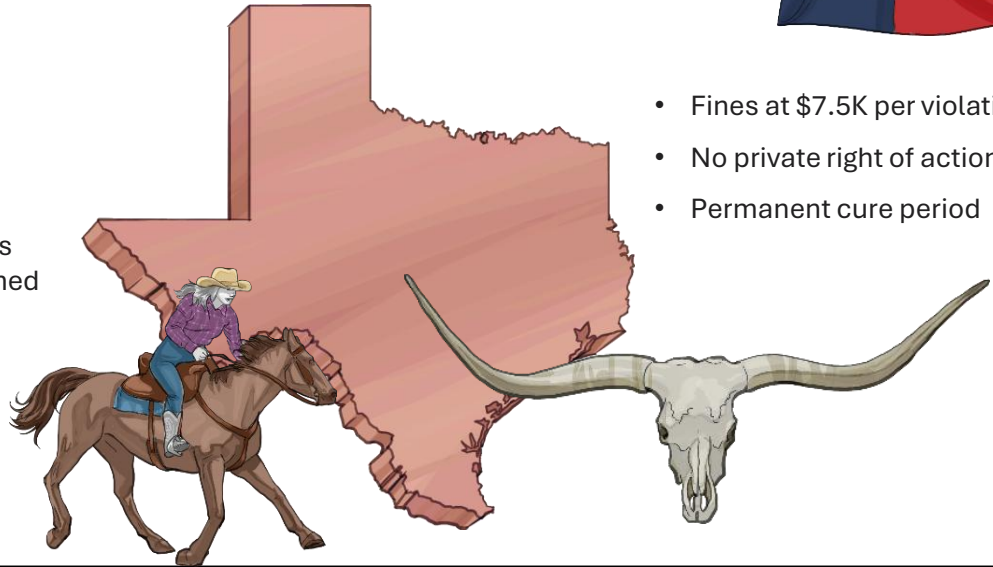
TEXAS

Data Privacy and Security Act



- Enacted in 2023
- Fairly standard law of its type
- Only one of a few laws to lack size or revenue applicability thresholds; instead, it exempts small businesses (as determined by the Small Business Administration)
- Standard list of sensitive data

- Fines at \$7.5K per violation
- No private right of action
- Permanent cure period

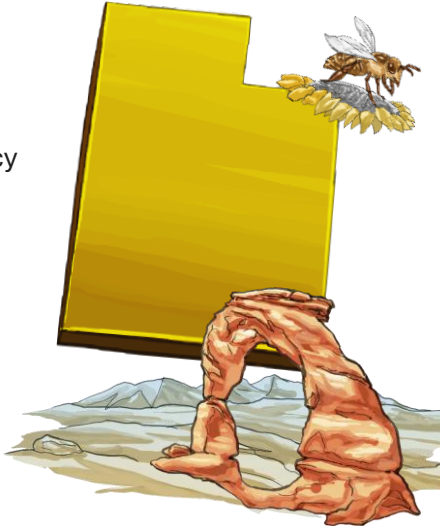


UTAH

Consumer Privacy Act



- Enacted in 2022
- High applicability threshold
- One of the weaker state consumer privacy laws
- Amended in 2025 to add a right to correction, joining all other states in having this right
- Amended in 2026 to apply to motor vehicle manufacturers that collect, transmit, or store personal data. Regular applicability thresholds don't apply.



- Short list of sensitive data
- Unlike most laws, no opt-in for sensitive data or DPIA requirement
- No DPIA requirement for anything
- No opt out right for profiling
- Fines at \$7.5K per violation
- No private right of action
- Cure period is permanent

SCOPE & APPLICABILITY

Extraterritorial

Applies when targeting products or services to Utah consumers.



Applies when business with revenue of \$25 million or more controls or process data on

- at least 100,000 UT residents; or
- at least 25,000 UT residents and derives 50%+ of gross revenue from sale of data

Applies to motor vehicle manufacturers that collect, transmit, or store personal data. Regular applicability thresholds don't apply.



Applies to for-profit companies.



Excludes data regulated by federal privacy laws such as HIPAA, GLBA, FCRA, and FERPA.

PERSONAL DATA



Identified



Identifiable



SENSITIVE DATA

Right to opt out of processing (unlike most states which require opt in and a DPIA)

Racial or Ethnic Origin



Religious Beliefs



Sexual Orientation



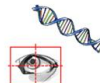
Geolocation Data



Mental or Physical Health History, Condition, or Diagnosis



Citizenship or Immigration Status



Genetic and Biometric Data



RESPONSIBILITIES FOR DATA PROCESSING

Notice



Data Minimization



Data Processing Agreements



Prohibition on Discrimination for Exercising Rights



Consent for Secondary Use



Data Security



Right to Opt Out

- targeted ads
- sale of data



Right to Know



Right to Access



Right to Correct



Right to Deletion



Right to Data Portability



INDIVIDUAL RIGHTS



ENFORCEMENT

Division of Consumer Protection investigates consumer complaints.



UT Attorney General enforces.



The Attorney General may recover actual damages to the consumer and an amount up to \$7.5K per violation.

No private right of action.



30-day cure period (permanent)

VERMONT

Data Privacy and Online Surveillance Act



- Enacted in 2026
- Long list of sensitive data. Includes transgender and non-binary status, neural data, government identifiers, financial info
- Narrower definition of “publicly available information” than many laws. Excludes data used to create a profile and inferences derived from the profile. Excludes genetic and biometric data collected without consumer’s knowledge, data shared with a restricted audience, nonconsensual intimate images.
- Applies to non-profits



- Provides for rights regarding profiling (being informed, questioning reasons, reviewing data)
- Fines at \$10K per violation
- No private right of action. An earlier version had one but was vetoed by the governor.
- Geofencing restrictions
- Right to cure will sunset



VIRGINIA

Consumer Data Protection Act



- Enacted in 2021
- Used as the model for most state consumer privacy laws
- Standard list of sensitive data
- Amended in 2025 to require opt-in consent to disclose, sell, or disseminate reproductive or sexual health information; has private right of action with statutory damages for violations of this provision



- Amended in 2026 to ban the sale of geolocation data
- Fines at \$7.5K per violation
- No private right of action (except for reproductive or sexual health info)
- Cure period is permanent

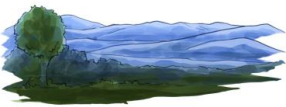
SCOPE & APPLICABILITY

Extraterritorial
Applies when targeting products or services to Virginia consumers.



The CDPA applies when business controls or process data on:

- at least 100,000 VA residents; or
- at least 25,000 VA residents and derives at least 50% of gross revenue from sale of data



Use Limitation



Data Protection Impact Assessments (DPIA)

- risk of harm
- targeted ads
- profiling
- sensitive data
- sale of data



Respond to Consumer Requests and Appeals Process
45 days to respond
+ 45-day extension



Prohibition on Discrimination for Exercising Rights



Right to Know



Right to Access



Right to Deletion



Right to Correction



Right to Opt Out

- targeted ads
- sale of data
- profiling



Right to Data Portability



PERSONAL DATA



Identified Identifiable

RESPONSIBILITIES FOR DATA PROCESSING



Data Processing Agreements



Data Minimization



Data Security



SENSITIVE PERSONAL DATA

Requires opt-in + DPIA to process.
Bans sale of geolocation data.

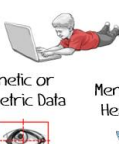


Requires opt-in consent to disclose, sell, or disseminate reproductive or sexual health info. Has private right of action with statutory damages for violations of this provision.

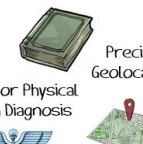
Racial or Ethnic Origin



Data Collected From Child



Religious Beliefs



Genetic or Biometric Data



Mental or Physical Health Diagnosis



Precise Geolocation



Sexual Orientation



Citizenship or Immigration Status



ENFORCEMENT

Enforced by the Virginia Attorney General.



No private right of action.



Max fine \$7,500 plus expenses and attorney's fees.

30-day cure period (permanent)



Last Updated June 2026



ABOUT THE AUTHOR

Professor **Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. One of the world's leading experts in privacy law, Solove has taught privacy and security law since 2000, has published 10+ books and 50+ articles, including the leading textbook on privacy law and a short guidebook on the subject. His LinkedIn blog has more than 1 million followers.



In 2010, Professor Solove founded **TeachPrivacy**, a computer-based privacy and security training company. TeachPrivacy now has a library of 180+ training courses and provides training to hundreds of organizations, including some of the largest companies in the world.

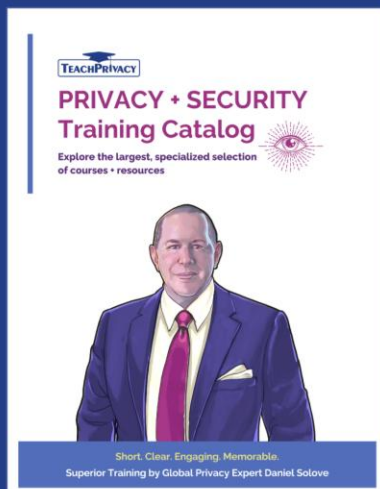
This guide and the whiteboards are personal use only. For distribution, use in presentations, use for institutional training, or use by compliance teams, please contact us at inquiry@teachprivacy.com.

Want More Resources Like This? Stay Connected with Professor Solove

Privacy Law Training

Bring Professor Solove's engaging, short privacy training programs to your organization. Explore our catalog of 180+ topics.

[Browse Catalog](#)



Free Privacy Newsletter

Get Professor Solove's free, weekly newsletter on privacy, AI, and tech issues. Expert analysis, cartoons, videos, events, and resources.

[Subscribe](#)

