

IAPP US State Comprehensive Privacy Laws Report

2023 LEGISLATIVE SESSION



Table of contents

What's inside?

Overview	3
Relevant definitions	10
Exemptions.....	13
Consumer rights	15
Business/controller obligations.....	19
Enforcement.....	28
Contacts	30



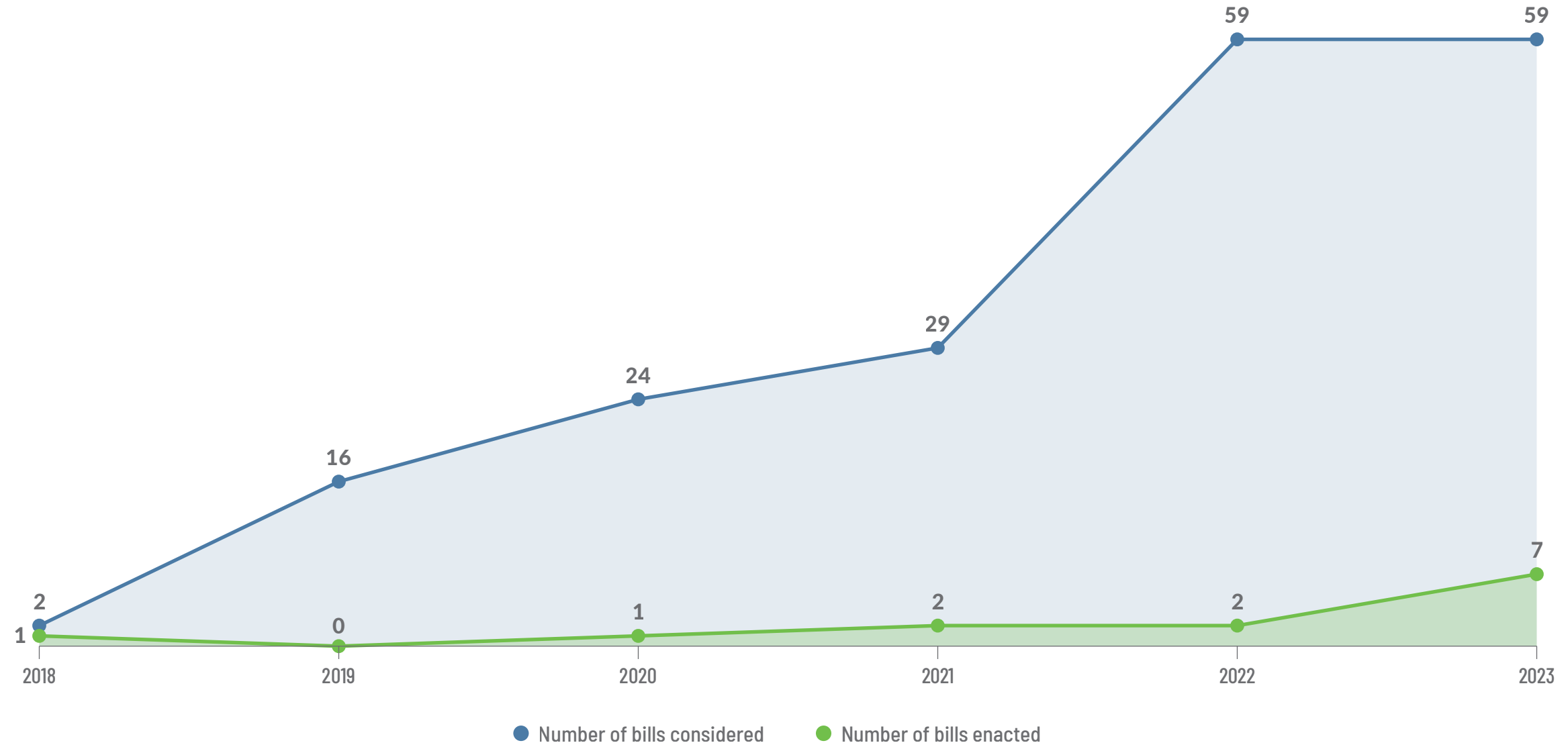
Overview

Keeping pace with US state privacy legislation

Each year since the passage of the California Consumer Privacy Act, the first comprehensive state law, in 2018, the number of proposed U.S. state privacy bills has increased. The IAPP aims to keep privacy professionals informed about when states introduce comprehensive privacy bills, when those bills progress into laws, what rights they offer consumers and what obligations they require from organizations.

In 2018, two bills were introduced in the U.S. and one became law in California. In 2019, 15 bills were introduced throughout the U.S. Of the 24 bills introduced in 2020, one was enacted, this time in the form of an update to the CCPA. In 2021, two of 29 introduced bills were enacted in Virginia and Colorado. In 2022, two of 59 introduced bills became laws in Utah and Connecticut. And in 2023, seven of 54 introduced bills became laws in Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Texas. Understandably, balancing compliance with passed laws while keeping track of newly introduced comprehensive privacy bills can be overwhelming for privacy pros. The IAPP [US State Privacy Legislation Tracker](#) provides a quick snapshot of new bills as each state's legislative session begins. This report provides a summary of relevant terms, applicability, exemptions, consumer rights, business obligations and enforcement duties for each of the 12 passed laws to date.

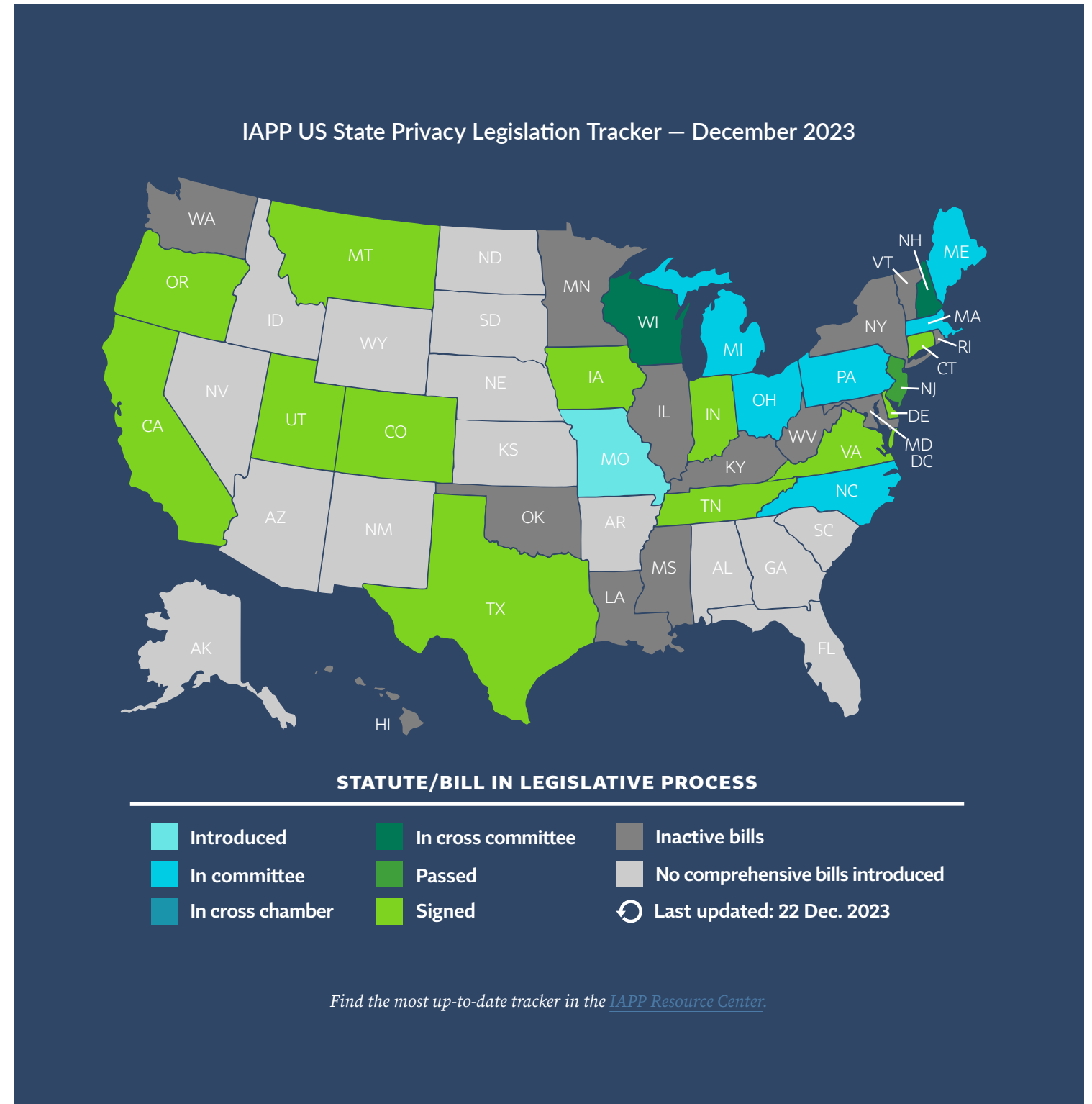
The growth of US state privacy legislation











Methodology

This report is limited to "comprehensive" U.S. state privacy laws that had been signed into law by 31 Dec. 2023. Bills that are sectoral, targeted at a particular industry or are use-case specific are purposely omitted. This decision necessarily excludes narrower state laws that are relevant to privacy, such as Florida's [Digital Bill of Rights](#) and Washington state's [My Health, My Data Act](#). While both of these laws, among others, may be applicable to the work of privacy pros, they are targeted at particular types of entities or types of data. Washington state's law, for example, regulates consumer health data.

Thus, to avoid comparing metaphorical apples to oranges, the analysis presented in this report, as well as in the IAPP US State Privacy Legislation Tracker, is limited to the U.S. state privacy laws the IAPP defines as "comprehensive," which carry omnibus sets of consumer rights and business obligations and apply to broad ranges of entities.



States with enacted laws

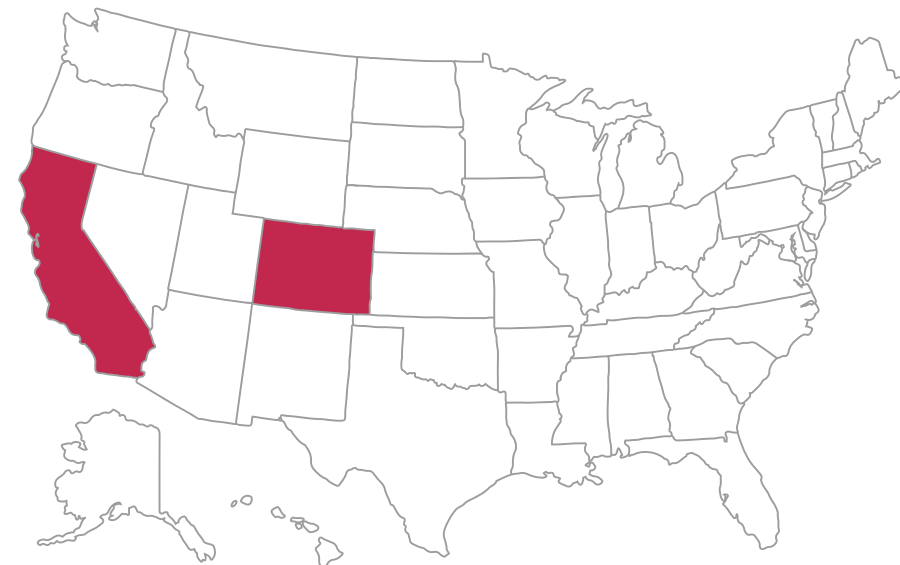
			
California California Consumer Privacy Act As amended by the: California Privacy Rights Act	Colorado Colorado Privacy Act	Connecticut Connecticut Personal Data Privacy and Online Monitoring Act	Delaware Delaware Personal Data Privacy Act
			
Indiana Indiana Consumer Data Protection Act	Iowa Iowa Consumer Data Protection Act	Montana Montana Consumer Data Privacy Act	Oregon Oregon Consumer Privacy Act
			
Tennessee Tennessee Information Protection Act	Texas Texas Data Privacy and Security Act	Utah Utah Consumer Privacy Act	Virginia Virginia Consumer Data Protection Act

Territorial scope

This report analyzes similarities and differences between the 12 enacted comprehensive U.S. state privacy laws. These states have continued to propose updates to the definitions, scopes and enforceability of their passed laws. As such, guidance continues to change with future amendments.

Just two states — Colorado and California — give rulemaking authority to the state attorneys general or privacy enforcement agencies. The Colorado attorney general's office released the finalized [Colorado Privacy Act Rules](#) 1 July 2023 to implement the Colorado Privacy Act. In California, the enforcement date of the new [CCPA Regulations](#) was pushed to March 2024.

States with rulemaking authority



CALIFORNIA AND COLORADO

Passage and enforcement dates of current US state privacy laws

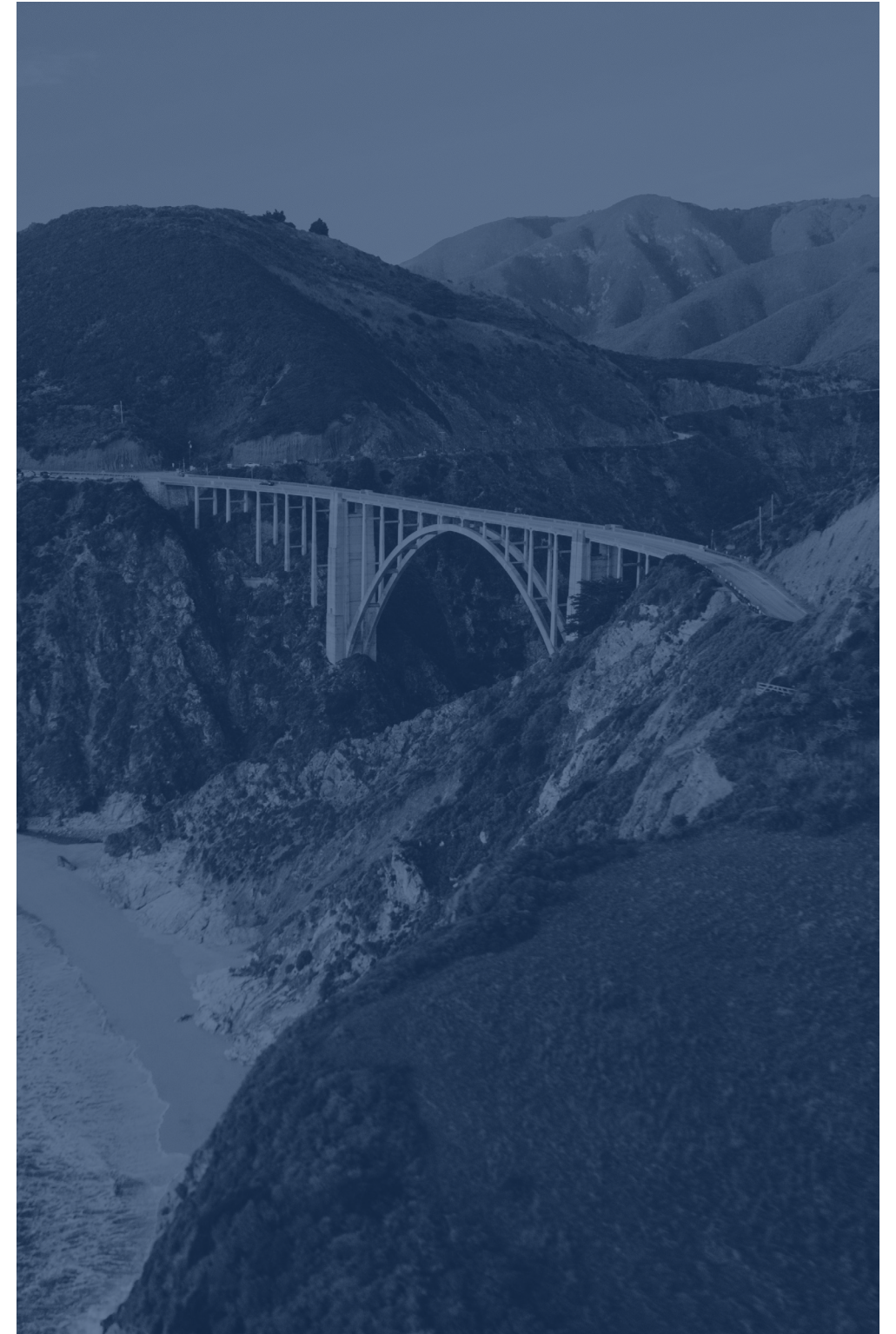
STATE PRIVACY LAW	DATE OF PASSAGE	DATE OF ENFORCEMENT
California Consumer Privacy Act	28 June 2018	1 Jan. 2020
California Privacy Rights Act	3 Nov. 2020	1 Jan. 2023
Virginia Consumer Data Protection Act	2 March 2021	1 Jan. 2023
Colorado Privacy Act	7 July 2021	1 July 2023
Connecticut Personal Data Privacy and Online Monitoring Act	10 May 2022	1 July 2023
Utah Consumer Privacy Act	24 March 2022	31 Dec. 2023
Oregon Consumer Privacy Act	22 June 2023	1 July 2024
Texas Data Privacy and Security Act	16 June 2023	1 July 2024
Montana Consumer Data Protection Act	19 May 2023	1 Oct. 2024
Iowa Consumer Data Protection Act	29 March 2023	1 Jan. 2025
Tennessee Information Protection Act	11 May 2023	1 July 2025
Indiana Consumer Data Protection Act	1 May 2023	1 Jan. 2026
Delaware Personal Data Privacy Act	11 Sept. 2023	1 Jan. 2025

	The California approach (CCPA/CPRA)	The Washington approach (e.g., VCDPA, UCDPA, CTDPA)
REQUIRES NOTICE AT COLLECTION	✓	✗
INCLUDES SENSITIVE DATA	Not in CCPA, but included in CPRA amendments	✓
LIMITS USE OF SENSITIVE DATA	✓	✗
CREATES A STATE PRIVACY AGENCY	✓	✗

Two differing approaches

So far, the U.S. has seen two different approaches to state consumer privacy laws. While California followed its own approach, the other states, at least initially, generally based their laws on a version of the yet to-pass Washington Privacy Act. For example, California uses the term "business," whereas the other states use the term "controller" for certain entities subject to the law, which may include an individual, corporation, business trust, nonprofit, and other legal and commercial entities.

At this point, California is also the only state requiring notice at collection. The CCPA initially did not address sensitive data, but this was updated by the CPRA amendments. With the CPRA amending the CCPA, California is now the only state that gives consumers the right to limit the use and disclosure of sensitive personal information. Also, unlike the other states, California is the only one with a dedicated privacy agency, the California Privacy Protection Agency.



Applicability of US state comprehensive privacy laws

	CCPA	CPRA	Colorado	Connecticut	Delaware	Indiana	Iowa	Montana	Oregon	Tennessee	Texas	Utah	Virginia
JURISDICTIONAL THRESHOLD	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state <i>(excludes small businesses)</i>	Doing business in the state and USD25 million in annual revenue	Doing business in the state
AND ONE OF THE FOLLOWING:													
REVENUE THRESHOLD	>USD25 million	>USD25 million	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PROCESSING THRESHOLD	50K+ consumers	100K+ consumers	100K+ consumers	100K+ consumers <i>(excludes payments data)</i>	35K+ consumers <i>(excludes payments data)</i>	100K+ consumers	100K+ consumers	100K+ consumers <i>(excludes payments data)</i>	100K+ consumers <i>(excludes payments data)</i>	100K+ consumers	Any processing of data	100K+ consumers	100K+ consumers
SALE THRESHOLD	50% of revenue from selling data	50% of revenue from selling or sharing data	Any revenue or discount from selling data and data of 25K consumers	25% of revenue from selling data and data of 25K consumers	20% of revenue from selling data and data of 10K consumers	50% of revenue from selling data and data of 25K consumers	50% of revenue from selling data and data of 25K consumers	25% of revenue from selling data and data of 25K consumers	25% of revenue from selling data and data of 25K consumers	50% of revenue from selling data and data of 25K consumers	Any sale of data	50% of revenue from selling data and data of 25K consumers	50% of revenue from selling data and data of 25K consumers

Relevant definitions

Defining privacy

The 12 states with comprehensive consumer privacy laws each define important terms like consumer, personal data and sale. Because each state law interprets these terms differently, it is important for privacy pros to understand the nuances in the definitions across the various state laws.

Terms with varying definitions in
US state comprehensive privacy laws



SALE



PERSONAL DATA



CONSUMER



SENSITIVE
PERSONAL DATA

Sale and consumer

The term sale is defined as "an exchange of personal data for monetary or other valuable consideration" in California, Colorado, Connecticut, Delaware, Montana, Oregon, Tennessee and Texas, while the definition only includes "monetary consideration" in Indiana, Iowa, Virginia and Utah. Of the existing state privacy laws, four define consumer as a resident of the state and exclude parties acting in a commercial or employment context. In California, however, consumers also include employees.



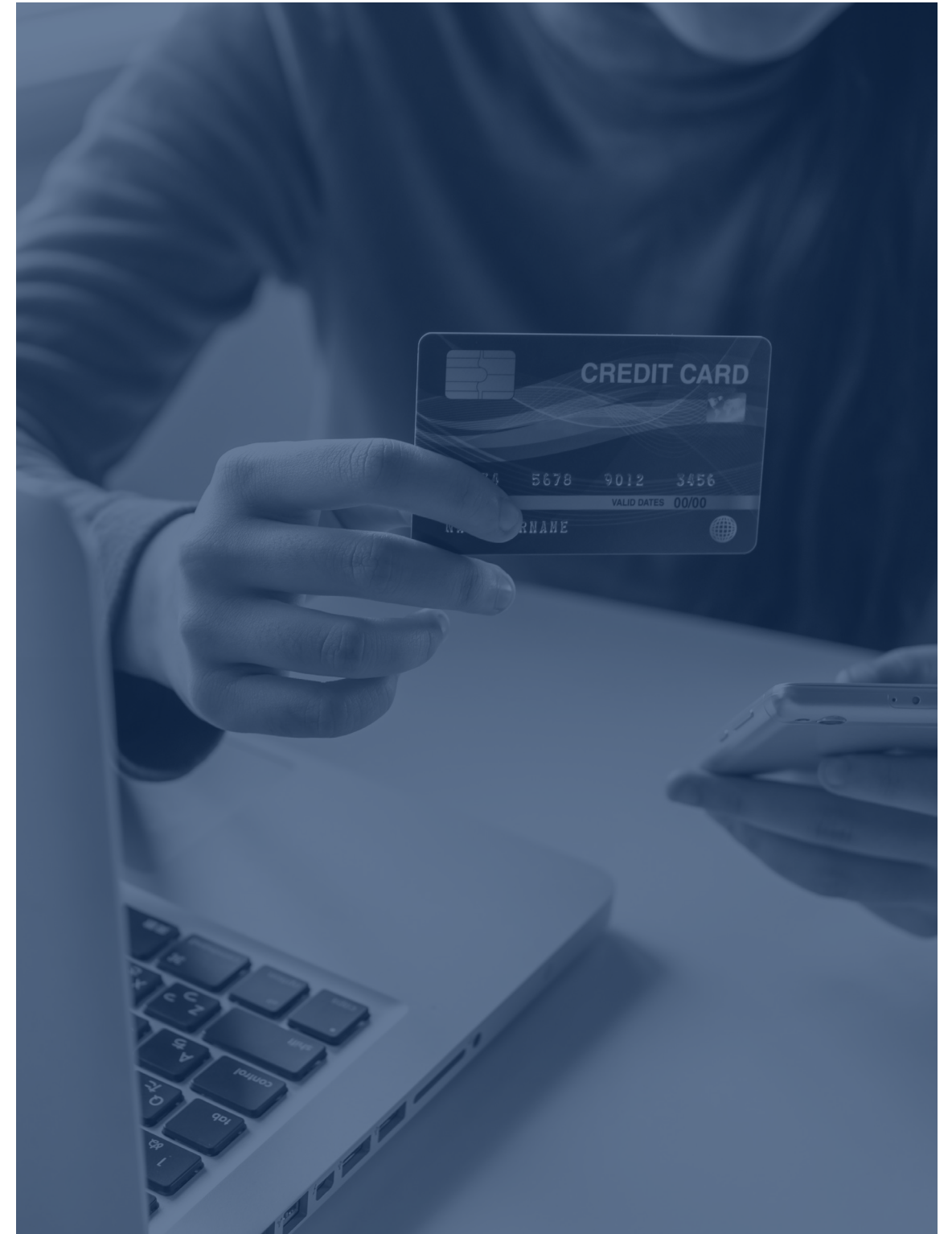
SALE

- Sale defined as "an exchange of personal data for..."
 - "...monetary or other valuable consideration" in California, Colorado, Connecticut, Delaware, Montana, Oregon, Tennessee and Texas.
 - "...monetary consideration" only in Indiana, Iowa, Virginia and Utah.



CONSUMER

- Most define consumer to exclude those acting in a commercial or employment context.
 - California does not exclude such individuals, and exemptions for this data expired 1 Jan. 2023.



Personal data and sensitive personal data

The comprehensive state privacy laws all exclude publicly available information and deidentified data from their definitions of personal data. California, Indiana, Iowa, Tennessee and Utah additionally exclude aggregate data.

All 12 states include consumer race or ethnic origin, religious beliefs, genetic data, biometric data, health data and sexual orientation, citizenship and immigration status in their definitions of sensitive personal data. Each law further clarifies biometric data, as evidenced by Virginia's exclusion of facial recognition technology data from its definition. The Colorado Privacy Act Rules define biometric data in a similar, but not identical, fashion as the other laws. In Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Virginia, sensitive data also includes personal data from known children. California, Colorado, Connecticut, Delaware and Montana include information about consumers' sex lives in the definition. All the states except Colorado include precise or specific geolocation data in their definitions of sensitive personal data. Delaware and Oregon specifically denote geolocation data as sensitive data if it accurately identifies an individual's present or past location within a radius of 1,750 feet. Lastly, the CPRA includes a few additional types of personal data: philosophical beliefs, union membership, account login information, government-issued identifications and contents of mail, email or text messages.



PERSONAL DATA

- All exclude publicly available information and deidentified data from the definition of personal data.
- California, Indiana, Iowa, Tennessee and Utah also exclude aggregate data.



SENSITIVE PERSONAL DATA

- All define sensitive personal data to include race or ethnic origin, religious beliefs, genetic data, biometric data, health data and sexual orientation.
- Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Virginia include personal data from a known child.
- Most include precise geolocation data.
- California includes additional categories, such as philosophical beliefs and the contents of a consumer's mail, email and text messages.



Exemptions

The two main exemptions

The 12 U.S. state privacy laws generally have two types of exemptions: one at the entity level and one at the data level. Most of the entity-level exemptions include government entities, nonprofits, and entities already regulated by the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act. There are two exceptions: Colorado does not provide an entity-level exemption for nonprofits or HIPAA-regulated entities and California does not provide an entity-level exemption for GLBA-regulated entities. Connecticut, Delaware, Indiana, Iowa, Montana, Tennessee, Texas, Virginia and Utah exempt higher education institutions, while Colorado, Connecticut, Delaware and Montana specifically exempt registered national securities associations.

All 12 states exempt data regulated under HIPAA, GLBA, the Fair Credit Reporting Act and the Driver's Privacy Protection Act. These exemptions also come with some exceptions. Colorado and Utah only exempt GLBA-regulated data if the entity is GLBA-compliant. Virginia, Utah and Connecticut only exempt DPPA-regulated data if the entity is DPPA-compliant. All the states except Colorado exempt data regulated by the Family Educational Rights and Privacy Act, and all but California exempt employee and commercial business-to-business data.

US state comprehensive privacy law exemptions



ENTITY LEVEL

- Most exempt:
 - Government
 - Nonprofits
 - HIPAA-regulated entities
 - GLBA-regulated entities
- Institutions of higher education exempt under laws in Connecticut, Delaware, Indiana, Iowa, Montana, Tennessee, Texas, Virginia and Utah.
- Registered national securities associations exempt under laws in Colorado, Connecticut, Delaware and Montana.



DATA LEVEL

- All state laws generally exempt data regulated under:
 - HIPAA
 - GLBA
 - FCRA
 - DPPA
- Most state laws exempt FERPA regulated data.
- Most state laws exempt employee data and commercial business-to-business data.

The background of the left page features a blue-tinted image of the Statue of Liberty holding the torch, with an American flag waving in the upper right corner. The text 'Consumer rights' is centered in white, flanked by two horizontal white lines.

Consumer rights

Access, portability, deletion, correction and opt-out

The CCPA set the standard for the rights consumers can expect from other state privacy laws. These consumer rights include the rights to access, port, delete and correct data, and opt out of sales or certain processing of data. All 12 states provide consumers the right to access their personal data, with Colorado and Connecticut providing an exception to this right if it requires a covered entity to reveal a trade secret. In the majority of states, covered entities are not required to disclose trade secrets when following the respective state privacy laws. The right to data portability is not consistently guaranteed. Indiana, Iowa, Montana, Tennessee, Texas, Virginia and Utah limit consumers' right to obtain a portable copy of their data to consumer-provided data only.

Similarly, the right to deletion comes with certain exceptions across state lines. In California, Iowa and Utah, consumers have the right to delete only consumer-provided data, while the remaining states allow consumers the right to delete any personal data the covered entity has concerning them. Virginia passed further amendments that provide an exemption to this right where the personal data was collected from a third-party source. All states but Iowa and Utah provide consumers with the right to correct inaccurate personal data the covered entity maintains about them. Finally, when it comes to opt out rights, all states provide consumers the right to opt out of sales and some form of targeted advertising. All states except Iowa and Utah also provide the right to opt out of profiling, and only California affords the right to limit the use and disclosure of sensitive personal information. However, in all states but California, Iowa and Utah, consumers must opt in before a covered entity processes their sensitive data.

Consumer rights

ACCESS AND PORTABILITY

Do ✓

ACCESS

- All states generally give consumers a right to access their data.
- Trade secrets are explicitly excluded in Colorado, Connecticut and California.

Do ↻

PORTABILITY

- Consumers have the right to data portability for:
- Only consumer-provided data in Indiana, Iowa, Montana, Tennessee, Texas, Virginia and Utah.
 - Any personal data the business/controller has concerning the consumer in California, Colorado, Connecticut, Delaware and Oregon.

Consumer rights

DELETION AND CORRECTION



DELETION

→ Consumers have the right to delete:

- Only consumer-provided data in California, Iowa and Utah.
- Any personal data the business/controller has concerning the consumer in Colorado, Connecticut, Delaware, Indiana, Montana, Oregon, Tennessee, Texas and Virginia.



CORRECTION

→ Most states give consumers a right to correct inaccurate personal data.

- Only Iowa and Utah do not provide this right.

Consumer rights

OPT-OUT RIGHTS



	California	Colorado	Connecticut	Delaware	Indiana	Iowa	Montana	Oregon	Tennessee	Texas	Utah	Virginia
SALES	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SHARED/ TARGETED ADVERTISING	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
PROFILING	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓

Note: There are definitional differences between the laws (e.g., sale).

Business/ controller obligations

Creating accountability for businesses

Comprehensive state privacy laws are not only passed to provide consumers with data rights, but also to create accountability measures for businesses — and nonprofits in the case of Colorado — that collect, use, process, own, manage and discard consumer data. State privacy laws include requirements for processing, treatment of children's data, transparency, data security, data protection assessments, nondiscrimination and consumer requests.

Business requirements under US state privacy laws



PROCESSING
RESTRICTIONS



TREATMENT OF
CHILDREN'S DATA



TRANSPARENCY



DATA SECURITY



DATA PROTECTION
ASSESSMENTS



NONDISCRIMINATION



CONSUMER REQUESTS

Requirements of covered entities

Notice and consent

All 12 states generally require covered entities to provide privacy notices, including information about how they use and process consumer data. California's notice-at-collection requirement ensures each covered entity notifies consumers about which categories of personal information are collected and the business purposes for doing so, along with a link to its "Do Not Sell" page and privacy policy. Colorado, Connecticut, Delaware, Indiana, Montana, Oregon, Tennessee, Texas and Virginia require consumer consent before processing sensitive data, while Iowa and Utah specifically require covered entities to provide notice and the opportunity to opt out of sensitive data processing. Interestingly, California and Connecticut require consent to sell, share or process the data of consumers under age 16 for targeted advertising purposes, while the other ten states require parental consent to process the data of consumers under age 13.

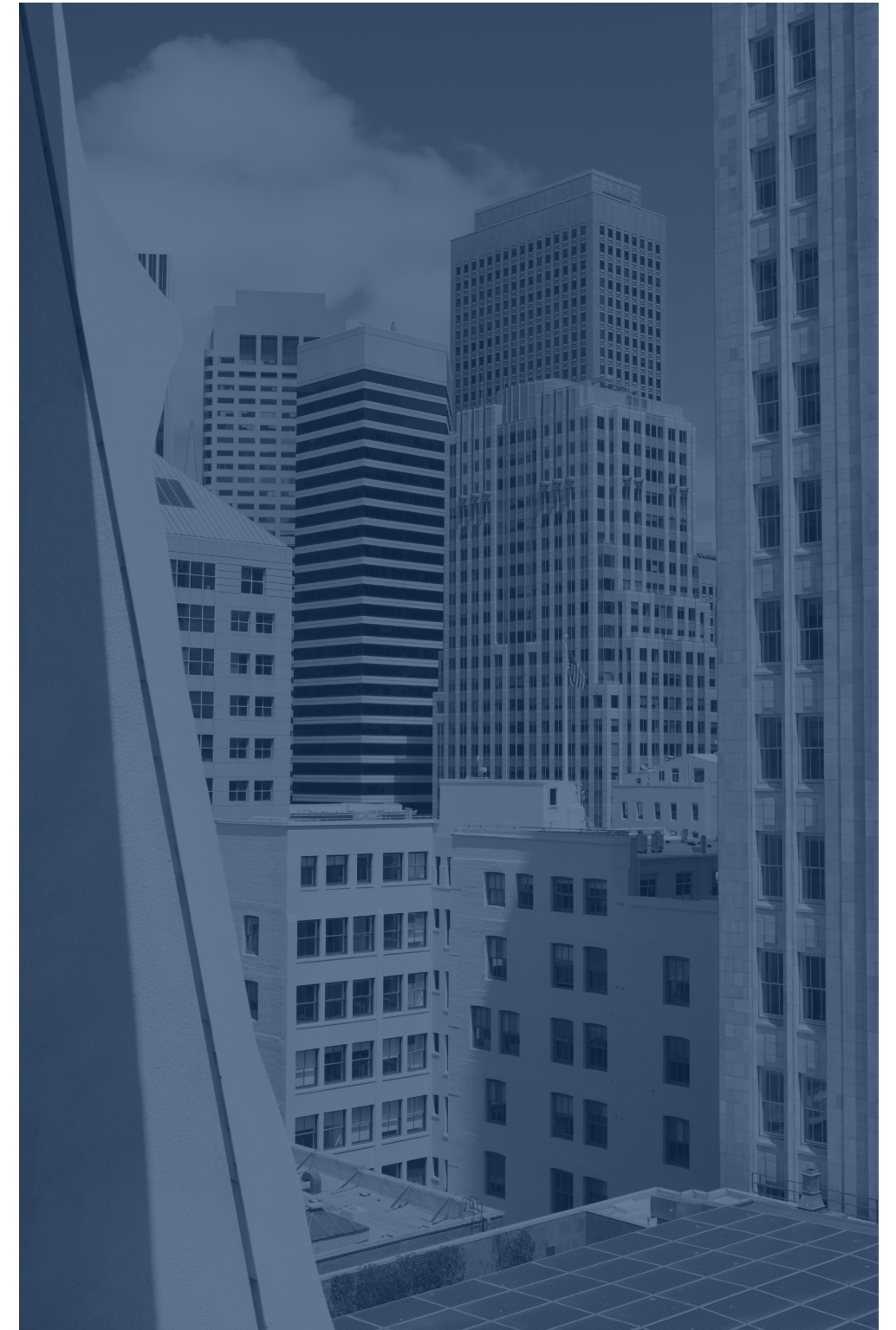
Responding to consumer requests

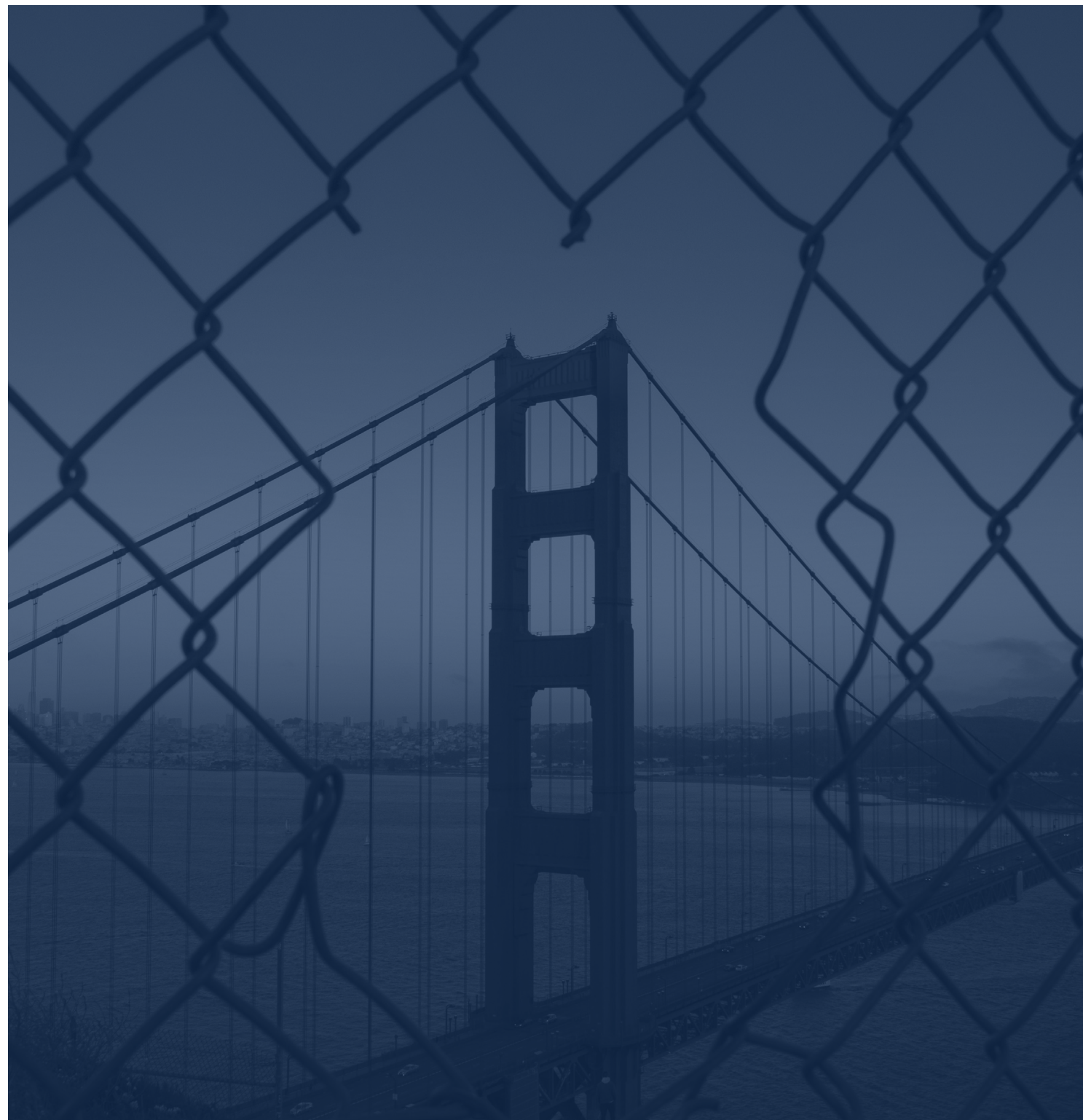
Most states provide general parameters for responding to consumer requests but leave the processing of those requests to the covered entity's discretion. Consumers must verify their identities when submitting requests to covered entities in Colorado, Montana, Virginia and Utah, but California, Connecticut, Indiana, Iowa,

Oregon, Tennessee and Texas do not require verification for opt-out requests. Separately, in California, Colorado, Delaware, Montana, Oregon and Texas, an authorized agent of a consumer may exercise the consumer's rights if their identity can be verified. All states but Iowa have a 45-day response period, while Iowa has a 90-day response period, during which covered organizations are expected to respond to consumer requests with the ability to extend the period if reasonably necessary. For opt-out requests, California and Connecticut specify a 15-day response period. Further, Colorado, Connecticut, Indiana, Iowa, Oregon, Montana, Tennessee, Texas and Virginia have appeals process requirements to help consumers contact their state attorneys general, and the Department of Justice in Delaware, if they are dissatisfied with appeal results.

Universal opt-out

A recent development among state privacy laws has been the recognition of universal opt-out mechanisms like Global Privacy Control. The CPRA amendments in 2020 required businesses to recognize universal opt-out mechanisms, which will also be required beginning 1 July 2024 in Colorado, 1 Jan. 2025 in Connecticut, Delaware, Montana and Texas, and 1 Jan. 2026 in Oregon.





Data security

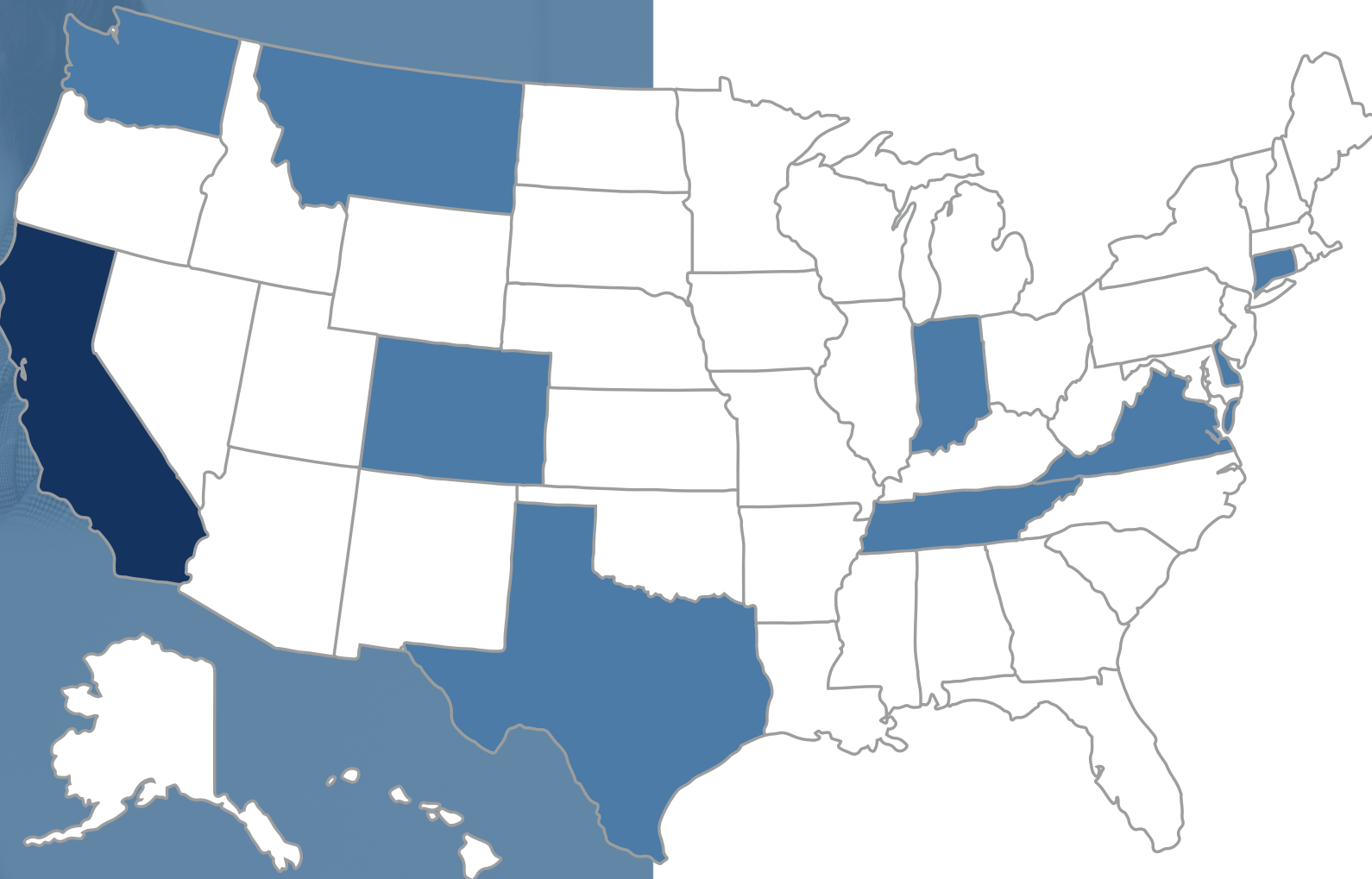
There is variation among U.S. state privacy laws regarding requirements to maintain reasonable data security practices. [California](#) relates its reasonable security to practices a covered entity takes that would be appropriate to the nature of the information requiring protection from unauthorized access, destruction, use, modification or disclosure. [Connecticut](#), [Delaware](#), [Indiana](#), [Iowa](#), [Montana](#), [Tennessee](#), [Texas](#) and [Virginia](#) go one step further, requiring "reasonable administrative, technical, and physical data security practices" to be appropriate to the volume and nature of the personal data at issue. In [Oregon](#) and [Utah](#), reasonable data security practices must not only protect the confidentiality and integrity of the personal data, but also reasonably reduce any foreseeable risks of harm to consumers, in an appropriate way for the controller's business size, scope, and type, and the volume and nature of the personal data. On the other end of the spectrum, [Colorado](#) places its explanation of reasonable security practices within a rule that describes the [duty of care](#).

Risk assessments

California, Colorado, Connecticut, Delaware, Montana, Oregon, Tennessee, Texas and Virginia require covered entities to conduct data protection or risk assessments for certain types of processing activities, like selling or processing personal data.

Business/controller obligations

PROCESSING RESTRICTIONS



- California has a notice-at-collection requirement. The CPRA limits the use and disclosure of sensitive data.
- Colorado, Connecticut, Delaware, Indiana, Montana, Oregon, Tennessee, Texas and Virginia require consent to process sensitive personal data, as defined by each law.

Business/controller obligations



UNDER 13 YEARS OLD

→ Consent is required to process data in:

- Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah and Virginia.



UNDER 16 YEARS OLD

→ Consent is required to sell, share or process data for targeted advertising purposes in:

- California and Connecticut.

TREATMENT OF CHILDREN'S DATA

Business/controller obligations

TRANSPARENCY AND DATA SECURITY



TRANSPARENCY

→ All states generally require privacy notices with certain information.



DATA SECURITY

→ All states generally require businesses/controllers to maintain reasonable data security.

Note: There is variation among the laws for what each obligation requires.

Business/controller obligations



ASSESSMENTS

- Most states generally require controllers to conduct data protection assessments for certain types of processing activities.
- Iowa and Utah do not require these assessments.



DISCRIMINATION

- All states generally prohibit discrimination against consumers for exercising their rights.

DATA PROTECTION ASSESSMENTS AND NONDISCRIMINATION

Business/controller obligations



AUTHENTICATION

→ Generally required for all consumer requests, except opt-out requests in California, Connecticut, Indiana, Iowa, Oregon, Tennessee and Texas.



UNIVERSAL OPT-OUT PREFERENCE SIGNALS

→ Recognized in California.

→ Will be recognized in Colorado 1 July 2024; in Connecticut, Delaware, Montana and Texas 1 Jan. 2025 and in Oregon 1 Jan. 2026.

RESPONDING TO CONSUMER RIGHTS REQUESTS



APPEALS PROCESS

→ Colorado, Connecticut, Delaware, Indiana, Iowa, Oregon, Montana, Tennessee, Texas and Virginia



TIMING

→ Iowa requires a 90-day response period.

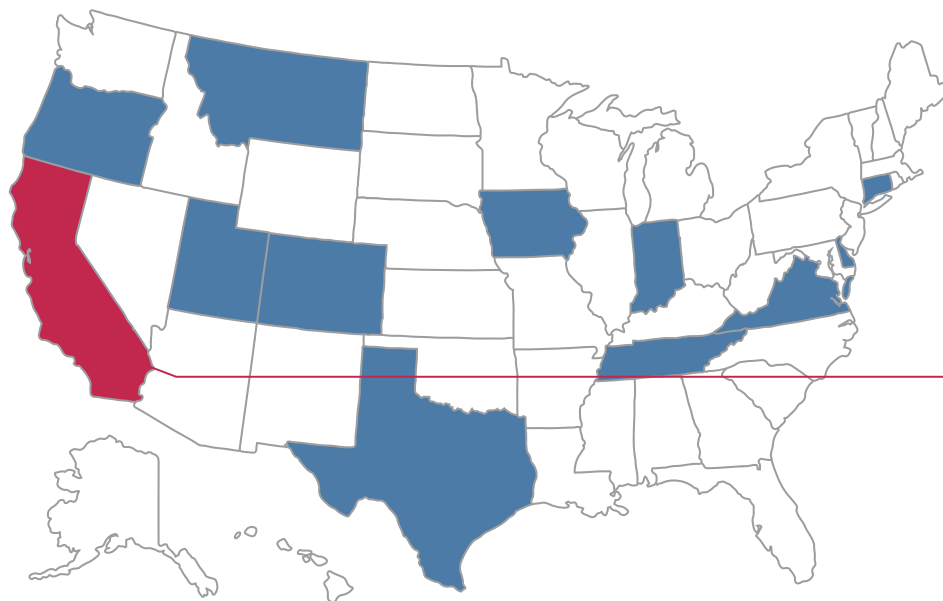
→ The remaining 11 states require a 45-day response period.

→ All states generally include discretionary extension.

Data processing agreements

All 12 states generally require data processing agreements between controllers and processors, or service providers as they are called under California law. California also requires these agreements for third parties under certain circumstances. There is variation among the laws with respect to what is required by the data processing agreements. Notably, in contrast to many global privacy laws, there are no restrictions on international data transfers in U.S. state consumer privacy laws.

Data processing under US state privacy laws



→ All 12 states generally require data processing agreements between controllers and processors.

→ California has specific contractual requirements for contractors, service providers and third parties.





Enforcement

Enforcement authority, cure periods and civil penalties

All states except Delaware utilize their attorneys general for enforcement purposes, while Delaware utilizes the Department of Justice. California places joint enforcement authority in its attorney general and the CPPA created by the CPRA, and Colorado places joint enforcement authority in its attorney general and district attorneys. Only California allows a private right of action, but it is limited to data breaches. The states generally provide a cure period, during which covered entities found to have privacy act violations can remedy issues before facing enforcement. Indiana, Oregon, Texas, Utah and Virginia offer 30-day cure periods, Colorado, Connecticut, Delaware, Montana and Tennessee offer 60-day cure periods, and Iowa offers a 90-day cure period. This feature is no longer provided in California, will sunset 1 Jan. 2025 in Colorado and Connecticut and 1 April 2025 in Montana, and has a contingency date of 1 Jan. 2026 in Delaware.

Covered entities that violate their respective state laws can face fines of USD2,500 per violation or USD7,500 per intentional violation or violation involving consumers under 16 in California, up to USD7,500 per violation in Indiana, Iowa, Oregon, Texas, Utah and Virginia, USD5,000 per willful violation in Connecticut, up to USD10,000 per violation in Delaware, up to USD15,000 per violation in Tennessee and up to USD20,000 per violation in Colorado. Unlike the other states, Montana's law does not specify a civil penalty.

Enforcement of US privacy laws



ENFORCEMENT AUTHORITY

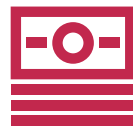
- Attorneys general in all states (except Delaware), but joint enforcement authority in:
 - California, with the CPPA.
 - Colorado, with district attorneys.
- Private right of action available only in California and limited to data breaches.



CURE PERIODS

- 30 days: Indiana, Oregon, Texas, Utah and Virginia.
- 60 days: Colorado, Connecticut, Delaware, Montana and Tennessee.
- 90 days: Iowa.

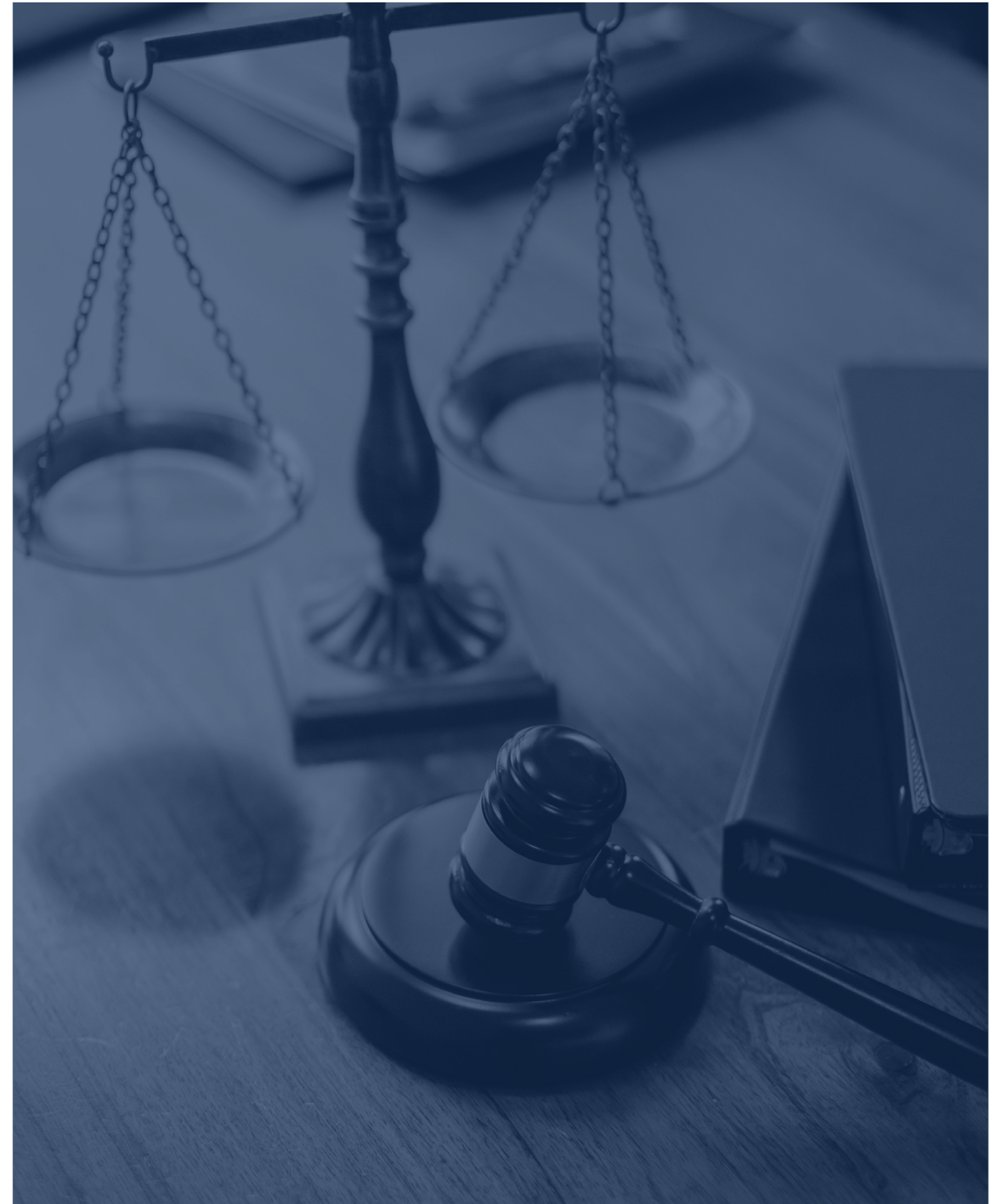
Note: the right to cure provisions will sunset in Colorado, Connecticut and Montana, and may sunset for certain entities in Delaware.



CIVIL PENALTIES

- Maximum fines per violation range from USD2,500-20,000.

Note: Montana does not specify a civil penalty.



Contacts

Connect with the team

Andrew Folks, CIPP/US
Westin Fellow, IAPP
afolks@iapp.org

**Anokhy Desai, CIPP/US,
CIPT, CIPM**
Former Westin Fellow, IAPP

Müge Fazlioglu, CIPP/E, CIPP/US
Principal Researcher, Privacy Law
and Policy, IAPP
muge@iapp.org

Joe Jones
Director of Research and
Insights, IAPP
jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media



Published January 2024.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2024 International Association of Privacy Professionals. All rights reserved.