

US State Privacy Law Tracker

Last updated: June 2022

California, Colorado, Virginia, Utah, and Connecticut all passed comprehensive privacy laws in recent years—creating a patchwork of requirements that companies must understand and abide by in order to avoid significant penalties.

Additional privacy legislation has been introduced in 26 other states, six of which are actively in committee, so understanding these laws and implementing stricter data privacy measures will soon be table stakes for operating a business in the US.

Read on to learn what each state privacy laws requires and how they will affect your business.

California Consumer Privacy Act (CCPA) <small>*As amended by CPRA</small>	Virginia Consumer Data Protection Act (VCDPA)	Colorado Privacy Act (CPA)	Connecticut Data Privacy Act (CTDPA)	Utah Consumer Privacy Act (UCPA)
Effective Date				
January 1, 2023	January 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023
Thresholds to Applicability				
CPRA Conducts business in CA and collects personal information of CA residents AND Fulfills one of the following: Shares, sells, or buys personal data for 100,000 or more consumers per year - Has \$25 million or more in annual revenue for the preceding calendar year - Earns more than 50% of annual revenue from selling or sharing personal information	VCDPA Conducts business in VA or markets products/ services to VA residents AND Controls or processes the personal data of 100,000 or more consumers per year OR Derives over 50% of gross revenue from selling personal data and processes the personal data of 25,000+ consumers	CPA Conducts business in CO or markets products/ services to CO residents AND Controls or processes the personal data of 100,000 or more consumers per year OR Derives any revenue or receives discounts from selling personal data and controls personal data of 25,000 or more consumers	CTDPA Conducts business in CT or markets products/ services to CT residents AND Controls or processes the personal data of 100,000 or more consumers per year OR Derives over 25% of gross revenue from selling personal data and processes the personal data of 25,000+ consumers	UCPA Conducts business in UT or markets products/ services to UT residents AND Has \$25 million or more in annual revenue AND Fulfills one of the following: Controls or processes personal data of 100,000 or more consumers per year - Derives over 50% of gross revenue from selling personal data and processes personal data of 25,000+ consumers
Consumer Rights				
Access Portability Deletion Correction	Access Portability Deletion Correction	Access Portability Deletion Correction	Access Portability Deletion Correction	Access Portability Deletion
Opt-in Consent				
Required to share or sell personal information for minors 16 years or younger	Required to process sensitive data	Required to process sensitive data	Required to share or sell personal information for minors age 13-16	Not required for sensitive data (unless the data concerns a child and parental consent is required)
Mechanism for Opt Out				
Required for sales, cross-contextual advertising, and automated profiling	Required for sales, targeted advertising, and automated profiling	Required for sales, targeted advertising, and automated profiling	Required for sales, targeted advertising, and automated profiling	Required for sales and targeted advertising
Data Protection Assessments				
Annual cybersecurity audit and risk assessments will be required—specific guidelines still to be determined	Required for sale, targeted advertising, sensitive data, and certain profiling	Required for sale, targeted advertising, sensitive data, and certain profiling	Required for sale, targeted advertising, sensitive data, and certain profiling	N/A
Authorized Agents				
Permitted for all consumer rights requests	N/A	Permitted for opt-out requests	Permitted for opt-out requests	N/A
Right to Appeal				
N/A	State must create an appeals process for consumers in the event a business refuses to fulfill consumer rights	State must create an appeals process for consumers in the event a business refuses to fulfill consumer rights	State must create an appeals process for consumers in the event a business refuses to fulfill consumer rights	N/A
Enforcement				
Attorney General and California Privacy Protection Agency	Attorney General	Attorney General District Attorneys	Attorney General	Attorney General <small>(All complaints vetted through Utah Division of Consumer Protection first.)</small>
Private Right of Action				
Yes, for security breaches involving specific sensitive personal information	N/A	N/A	N/A	N/A
Automatic Cure Period				
30-day cure period <small>(Discretionary as of Jan. 1, 2023)</small>	30 days	60 days <small>(Discretionary as of Jan. 1, 2025)</small>	60 days <small>(Discretionary as of Jan. 1, 2025)</small>	30 days
Fines				
Up to \$2,500 per unintentional violation or up to \$7,500 per intentional violation	Up to \$7,500 per violation in civil penalties	Up to \$20,000 per violation in civil penalties	Up to \$5,000 per violation in civil penalties	Up to \$7,500 per violation in civil penalties, plus actual damages to the consumer

Brought to you by Transcend

Transcend makes it easy to future-proof privacy compliance.

Transcend is a privacy infrastructure platform that helps companies like Robinhood, Patreon, and Clubhouse fulfill modern data rights with automated, easy-to-use solutions for **privacy request fulfillment, consent management, and data mapping**. We empower tech leaders to stay ahead on privacy compliance and build stronger relationships with their customers through respectful and compliant data transparency, consent, and control.

With Transcend's industry-leading privacy solutions, your company can go beyond patchwork compliance and manual processes—paving your way to the future of privacy.