

# Publications

## California Privacy Law Update: New Year, New Privacy Resolutions

### Related Professionals

[John L. Landolfi](#)

[Christopher L. Ingram](#)

[Christopher A. LaRocco](#)

[Gretchen Rutz Leist](#)

[Celina J. Needle](#)

### Related Services

[Data Strategy, Privacy and Security](#)

**CLIENT ALERT** | 12.19.2025

Though Colorado, Texas, and other states have been active in enacting new privacy protections in the past year, California continues to lead the way in U.S. privacy regulation. With key provisions of the Delete Act set to take effect on January 1, 2026, alongside other recent updates to California privacy laws and regulations, businesses operating in or serving California residents will encounter new compliance challenges in the new year. To help navigate California's ever-evolving privacy landscape, companies should consider the following "resolutions" for 2026 for businesses subject to these laws.

### Resolution 1: Don't DROP the Ball

Over the past year, data brokers and potential data brokers have registered with the California Privacy Protection Agency (**CalPrivacy**) to avoid hefty fines for failure to comply with California's **Delete Act**. A "data broker" broadly includes any business that "knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship," leaving many businesses still uncertain whether they qualify.

The Delete Act phases in additional compliance steps in 2026, including a centralized platform for Californians to request deletion of their personal data from all registered data brokers at once. CalPrivacy intends to launch the Delete Request and Opt-out Platform (**DROP**) by January 1, 2026, and data brokers must create a DROP account, complete registration, and pay an annual fee by January 31, 2026.

Starting August 1, 2026, data brokers must check the DROP every 45 days for consumer deletion requests. Data brokers are responsible for comparing such requests to their own records and deleting any matching consumer information. After a consumer's data is deleted, brokers must report the status of the deletion request in the DROP, ensure the consumer's data remains deleted, and not collect or sell new data about that consumer without consent.

The Delete Act imposes fines of \$200 per day for failure to register and fines of \$200 per day per consumer for failure to delete consumer information.

## Resolution 2: Think Before Taking Risks

The impact of the California Consumer Privacy Act, as amended by the California Privacy Rights Act (**CCPA**), continues to grow with ever evolving amendments to the CCPA regulations. While most of the significant changes regarding mandatory cybersecurity audits and disclosure and processing requirements for Automated-Decision Making Technology (**ADMT**) won't go into effect in 2026, new risk assessment measures go into effect January 1 of the new year. Starting January 1, 2026, businesses must conduct formal risk assessments before processing personal information in a manner that presents a "significant risk" to consumer privacy. "Significant risks" include: selling or sharing personal information, processing sensitive personal information, using ADMT for significant decisions concerning consumers, using automated processing to infer characteristics about a consumer (a) when acting in their capacity as an educational program applicant, job applicant, student, employee, or independent contractor; or (b) based on their presence in a sensitive location, or processing personal information for the purposes of training an ADMT to make significant decisions or for recognizing a person (e.g. facial recognition).

Businesses must submit information concerning risk assessments conducted in 2026 and 2027 to CalPrivacy by April 2028.

## Resolution 3: Know Your Boundaries

Effective January 1, 2026, businesses will also be prohibited from collecting, using, selling, or sharing the personal information of anyone located at or near family planning centers, except when necessary to provide requested services. It also prohibits geofencing around health care facilities for tracking, data collection, or targeted advertising, with limited exemptions for facility operations, certain research, labor activities with consent, and HIPAA-covered entities. Importantly, the amended law allows California residents to bring a civil action to recover damages and injunctive relief.

## Resolution 4: Stick to the Schedule

Also effective January 1, 2026, California will have stricter timelines for businesses to report data breaches to consumers and the California Attorney general. This new timeline requires businesses to notify California residents within 30 days of discovering a breach. In instances where over 500 California residents are notified, the business must also notify the California Attorney General within 15 days of notice to affected residents.

## Resolution 5: Remember Who You Are

California has also introduced several business-specific requirements. For example, effective January 1, 2026, social media platforms with more than \$100 million in gross annual revenue are required to provide a clear and conspicuous "Delete Account" button on the platform's settings menu. As another example, AI developers have been the target of several new California laws. Other specific requirements pertain to employee privacy and children's privacy. Businesses should make sure to review sector-specific privacy

laws for application.

