Stay Current

PAUL HASTINGS

December 2025

Follow us on LinkedIn

Regulatory Update

Plan Ahead: Updated CCPA Regulations Go Into Effect Jan. 1

By Aaron Charfoos, Michelle Reed and Brianne Powers

As we previously wrote, in September the California Office of Administrative Law (OAL) officially approved the California Privacy Protection Agency's (now CalPrivacy) long-awaited regulations pertaining to cybersecurity audits, risk assessments, automated decision-making and other subjects. The updated regulations help further CalPrivacy's objectives of providing Californians with robust privacy rights and protecting sensitive personal information, such as health and children's data.

As further expanded upon by CalPrivacy here, the requirements generally fall within the following categories (please note, while the updated regulations become **effective on Jan. 1, 2026**, the deadlines for certain requirements are not until much later, as we have highlighted below*)*:

1. **Risk Assessments, Cybersecurity Audits and Automated Decision-Making Technologies:** Businesses must conduct detailed risk assessments *before* engaging in activities such as selling or sharing personal information, processing sensitive personal information, and using or training certain automated technologies. Businesses whose processing of consumer personal information presents a "significant" risk to consumers' security must conduct an *annual* cybersecurity audit. Businesses should ensure they have mechanisms in place to capture these activities prior to their start (e.g., through training and awareness to product and marketing groups and required project documentation) and ensure that they have an established risk matrix upon which to assess inherent privacy risks to consumers.

    - **Risk Assessment Deadlines**: Businesses conducting risk assessments in 2026 and 2027 must submit information about the risk assessment to CalPrivacy by April 1, 2028. Information regarding risk assessments conducted after 2027 is due by April 1 of the following year.
    - **Cybesecurity Audit Deadlines**: Businesses are required to start conducting cybersecurity audits based on their revenue. A business with gross revenue over $100 million in 2026 must complete and submit an audit to the CPPA by April 1, 2028, covering the period from Jan. 1, 2027, through Jan. 1, 2028. A business with gross revenue over $50 million in 2027 must complete and submit an audit by April 1, 2029, covering the period from Jan. 1, 2028, through Jan. 1, 2029. A business with gross revenue under $50 million in 2028 must complete and submit an audit by April 1, 2030, covering the period from Jan. 1, 2029, through Jan. 1, 2030.
    - **Automated Decision-Making Technology Deadlines**: Businesses using automated decision-making technology for significant decisions must provide notice of such use at *or before point of collection* by Jan. 1, 2027.

2. **Confirmation of Opt-Out**: Businesses must provide a means by which a consumer can confirm the status of their opt-out request, including those submitted through an opt-out preference signal, like the Global Privacy Control (GPC). Not only must businesses ensure they have their GPC recognition functioning properly, but they must also give consumers reassurance that their opt-out has been received and honored. Businesses may choose to meet this requirement by implementing a new "pop-up" or flag to consumers when they initiate the opt-out.

3. **Requests to Know**: Consumers will have the ability to request access to all their personal information, going back as far as Jan. 1, 2022. This highlights the need to ensure that consumer personal information is properly accounted for and deleted when no longer necessary. Businesses should have established data retention policies and practices related to the secure deletion of information when appropriate.

4. **Requests to Correct/Requirements to Maintain Correct Data/Ability to Correct Health Data**: Businesses must be able to provide consumers with the sources from which they received any inaccurate information, including noting where the business itself is the source of the inaccurate information. Businesses must also maintain the corrected information going forward — this means that the information cannot be overridden in the future with inaccurate information (particularly where data brokers are in use). Finally, consumers will have the right to submit a 250-word statement contesting the accuracy of any health information where a business has denied a request to correct such health information. This statement must be made available by the business to others who have received such health information. These requirements further highlight the need for businesses to establish procedures for intaking, documenting and retaining information received from other sources and for ensuring that such information is accurate and up to date.

5. **Sensitive Personal Information**: The regulations define the personal information of consumers under 16 years old as sensitive personal information, subject to the rights of consumers to limit the use of such information. Businesses that regularly collect and maintain youth personal information will need to ensure their processes are able to honor such requests when received.

Relatedly, CalPrivacy will also launch the Delete Request and Opt-Out Platform (DROP) in January 2026. This system will allow California residents to delete their personal information collected, used and shared by data brokers, via a single-step process. Starting Aug. 1, 2026, data brokers will be required to access the DROP system to retrieve consumer requests that match their records at least once every 45 days. While some legal exemptions may apply, the data broker must delete all personal information associated with the requesting consumer within 45 days of receipt and maintain records of such requests going forward.

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises companies on the applicability of and compliance with state privacy laws and regulations, like the California Consumer Privacy Act (CCPA). If you have any questions concerning CCPA compliance, these regulations or the DROP requirements, please do not hesitate to contact a member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Dallas

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

Washington, D.C.

Brianne B. Powers
+1-202-551-1237
briannepowers@paulhastings.com