



FACT SHEET

DRAFT RISK ASSESSMENT REGULATIONS



The California Consumer Privacy Act (CCPA) directs the Agency to make rules requiring certain businesses to conduct risk assessments. The Agency has drafted risk-assessment regulations but has not started the formal rulemaking process. This fact sheet explains the draft regulations to help people understand and participate in the rulemaking process. These draft rules are *not* in effect and are subject to change.

WHO would need to conduct a risk assessment?


A “business” that must comply with the CCPA¹ would have to conduct a risk assessment before it does any of the following:

- 1 Sells or shares consumers’ personal information.**
- 2 Collects, uses, discloses, retains, or otherwise processs consumers’ “sensitive personal information.”²**
- 3 Uses automated decisionmaking technology (ADMT) for a “significant decision” or for “extensive profiling.”**
 - “ADMT” is technology that makes decisions, or that a person relies upon to make a decision (e.g., a resume-screening tool that a business uses to determine which applicants it will hire).
 - “Significant decisions” are decisions that have important consequences for consumers (e.g., decisions to provide or deny financial services, housing, insurance, educational or employment opportunities, healthcare services, or essential goods or services like groceries, medicine, or fuel).
 - “Extensive profiling” includes analyzing consumers’ personality, interests, behavior, or location in their workplace, at school, or in public places (e.g., using facial-recognition technology in a store to identify potential shoplifters), or to target ads to them.
- 4 Uses personal information to train ADMT or artificial intelligence (AI) that could be used:**
 - To identify people (e.g., facial-recognition technology);
 - For physical or biological identification or profiling (e.g., analyzing people’s facial expressions or gestures to infer their emotional state);
 - To make significant decisions;
 - To generate deepfakes (e.g., fake images of real people that are presented as truthful or authentic); or
 - To operate generative models.



WHAT would a risk assessment include?

- Why the business needs to do any of activities listed above.
- The types of personal information the business would collect, use, disclose, and retain to do the activity.
- How the business would do the activity (e.g., how many consumers would be affected, what the business would tell them about its use of their personal information, who else might be involved, which technology it plans to use; and for certain uses of ADMT, how the business would use the ADMT to make decisions).
- The benefits and consequences to consumers associated with the activity, and protections the business plans to put in place.

- 
- Benefits include benefits to the business, consumers, other stakeholders, and the public.
 - Consequences to consumers might include, for example, unauthorized access to their personal information, discrimination on the basis of protected characteristics (e.g., race or gender), not providing enough information to consumers so that they understand how their personal information would be used, or creating additional costs for consumers.
 - Examples of protections include encryption and privacy-enhancing technologies. A business using ADMT for a significant decision or extensive profiling would also have to identify whether it evaluated the ADMT to ensure it worked as intended and did not discriminate, and which accuracy and nondiscrimination safeguards it planned to put in place.

- The people at the business who contributed to, reviewed, and approved the risk assessment.
- Whether the business will initiate the activity.



Note: A business would not be allowed to start an activity if the risks to consumers' privacy outweighed the benefits of the activity.

WHEN would a business have to conduct or update a risk assessment?

A business would have to do a risk assessment before it started any of the activities listed above. It would also have to review (and update if needed) its risk assessments at least once every three years to make sure they remained correct.

If something important changed about how the business did the activity (e.g., if it needed to collect more sensitive personal information), the business would have to immediately update its risk assessment.



RISK



How would a business complete its risk assessment if it used service providers or contractors to conduct the activity?

The business's service provider or contractor would be required to give the business the information needed to conduct the risk assessment. A business could get information from them as part of its risk-assessment process.

WHAT would a business have to submit to the Agency, and WHEN?

A business would have 24 months to submit to the Agency: (1) a certification that it did its risk assessments as set forth in the draft regulations; and (2) abridged risk assessments.



What is an “abridged risk assessment”?

An abridged risk assessment is a shorter version of the full risk assessment. It would include which activity triggered the risk assessment; why the business needed to do that activity; the types of personal information needed for the activity and whether they included sensitive personal information; and the protections put in place.

After its first submission, the business would submit its certification and any new or updated abridged risk assessments annually.

If the Agency or the Attorney General requested a business's unabridged risk assessment, the business would have 10 business days to provide it.

What if a business did a risk assessment for the same activity to comply with other laws? Would that count toward its CCPA risk assessment?

A business would not have to redo the same risk assessment. However, if the risk assessment did not meet all of the requirements in the draft regulations, the business would have to add to it as needed.

¹ The CCPA generally does not apply to nonprofit organizations or government agencies. For more information, see “Does My Business Need To Comply With The CCPA?” fact sheet at <https://cppa.ca.gov/resources.html>.

² Sensitive personal information includes things like Social Security numbers, financial information, precise geolocation, health information, and children's personal information. For more information, see Civil Code § 1798.140(ae); Draft Update to Existing Regulations, March 2023, at § 7001(ii), available at https://cppa.ca.gov/meetings/materials/20240308_item4_draft_update.pdf, (including the addition of “[p]ersonal information of consumers that the business has actual knowledge are less than 16 years of age” to the definition); and “What is Personal Information?” fact sheet, available at: <https://cppa.ca.gov/resources.html>.

Supporting Resources: Civil Code § 1798.185(a)(15)(B); Draft Risk Assessment and Automated Decisionmaking Technology Regulations, March 2024, available at https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf.