BCLP. Client Intelligent

Insights

RISK ASSESSMENTS UNDER THE CCPA: KEY TRIGGERS, TIMELINES, AND COMPLIANCE STEPS

May 19, 2026

As we head into the second half of 2026, companies have had several months to digest and begin addressing the updated California Consumer Privacy Act ("CCPA") regulations. Among other requirements, Article 10 of these updates gives shape to the CCPA's general obligations regarding risk assessments, setting out timing requirements as well as the triggers and content obligations. Below, we provide an overview of the key aspects of these risk assessment requirements, beginning with the applicable timing obligations.

Timing and Retention Requirements

Although there is some nuance to the timing requirements, the high level takeaway is that companies need to start preparing their risk assessments and considering how to build the process into their broader privacy compliance strategy.

- If a particular processing activity occurred **before January 1, 2026**, organizations are required to conduct risk assessments no later than **December 31, 2027**.
- For any processing activity initiated on or after **January 1, 2026**, organizations are required to conduct the risk assessment **before** commencing the relevant activity.

In either case, the company must then submit the attestation and summary described below by **April 1, 2028**. Risk assessments must be reviewed and updated either every **three years** or within **45 days** whenever a material change to the processing activity is made.

Beginning on January 1, 2027, organizations must submit their attestation and summary by April 1 of the following year.

Businesses must maintain risk assessments for so long as the processing continues or for **five years** after the completion of the risk assessment, whichever is later.

Stakeholder Involvement

All employees whose job duties include participating in the processing of the personal information that is subject to a risk assessment must be included in the risk assessment process for that processing activity. For example, an individual who determines the method by which the business plans to collect consumers' personal information must provide that information to the individuals conducting the risk assessment. This is a mandatory obligation, not a matter of discretion, and businesses should ensure that relevant personnel are identified and engaged at the outset of the assessment process rather than as an afterthought.

Risk Assessment Triggers

Businesses are required to conduct risk assessments when they engage in processing activities that present a "significant risk" to consumer privacy. Such activities include:

- Selling or sharing personal information (which would include the use of personal information for targeted advertising—such as cookie-based tracking or CRM-based audience targeting—without express opt-in consent).
- Processing sensitive personal information (excluding processing of sensitive personal information for standard employment purposes, such as compensation payment, administering benefits or providing reasonable accommodations).
- Processing personal information with the intention of using it to train Automated Decision-Making Technology ("ADMT") for significant decisions concerning consumers or to train biometric technology.
- Using ADMT to make significant decisions regarding consumers (e.g., decisions regarding financial or lending services, housing, education, employment, or healthcare services).
- Using automated processing to infer or extract consumer characteristics based on systematic observation when a consumer acts in certain capacities and/or based on a consumer's presence in a sensitive location.

The Balancing Test: Risk Assessment Requirements

The purpose or goal of risk assessments is for organizations to evaluate whether the risks of the underlying processing activity to consumer privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public at large. Practically speaking, organizations need to establish through their risk assessment that the benefits do outweigh the risks. If the balancing test suggests otherwise, they will need to consider modifications or mitigation to tip the scale in favor of the underlying benefits.

In performing this balancing test, qualifying businesses must consider and include the following factors in their risk assessment reports:

- The categories of personal information that will be processed, including any categories of sensitive personal information. The personal information gathered must be limited to the minimum information necessary to achieve the relevant purpose(s) of processing.
- The purpose of processing the personal information (in specific rather than generic terms, such as “improving the services” or “in accordance with customer agreements”).
- How the business will process, retain, and use that personal information (i.e., the planned method for collecting the personal information).
- The retention period for each category of personal information.
- The business’s method of interacting with impacted consumers (e.g., websites, mobile apps, offline).
- The approximate number of consumers whose personal information the business plans to process.
- What disclosures the business has made or plans to make to the consumers about the processing of their personal information and how these disclosures were or will be made (e.g., via a just-in-time notice).
- The names or categories of the service providers, contractors or third parties to whom the business discloses or makes available personal information and the purposes of such disclosures.
- For ADMT, the logic of the ADMT and the output of the ADMT.
- The safeguards the business will employ in processing the personal information.
- The benefits of processing the personal information.
- The negative impacts on consumers’ privacy that will result from processing the personal information.
  - The regulations provide a number of examples of potential negative impacts including unauthorized access, destruction, use, modification or disclosure of personal information; discrimination based on protected characteristics; impairing consumers’ control of their personal information; coercing or compelling consumers into allowing the processing of their personal information; economic, physical, reputational, or psychological harm.
- Whether the business will begin the processing subject to the assessment.
- The individuals who provided the information for the risk assessment (not including those who provided legal advice).

- The date the assessment was reviewed and approved, as well as the names and positions of the individuals who reviewed or approved it.

Importantly, while qualifying businesses are required to conduct these assessments and compile this information, they may be able to use a risk assessment previously prepared for another purpose (i.e. to satisfy the requirements of the GDPR or another state's privacy law) instead, so long as the earlier assessment also satisfies the requirements set forth in the CCPA regulations.

Attestation Requirement

In addition to conducting and documenting risk assessments, organizations must submit an attestation and summary of risk assessments to the California Privacy Protection Agency (the "CPPA," also known as CalPrivacy) by April 1 of the year after the processing activity is initiated and the risk assessment is prepared, starting on April 1, 2028. The attestation and summary must outline the type of risk assessments conducted, the number of assessments conducted, and the categories of personal information involved, among other things. It must also affirm that the company did, in fact, conduct a risk assessment for the processing activities outlined in the regulations. The individual submitting the report must have the requisite authority to do so, be a member of the executive management team directly responsible for risk-assessment compliance, and have sufficient knowledge of the risk assessments to provide accurate information.

The Attorney General of California and the CPPA can also request specific risk assessment reports from organizations at any time; if they do, the report is due within thirty days of the request.

How to Get Started

Because companies are now required to conduct risk assessments for qualifying activities, there is no time to delay in setting up a process for identifying when an assessment must be conducted and for working through the process. To kick off this process, companies subject to the CCPA should take the following steps:

- Identify processing activities (either already happening or anticipated) that present a "significant risk" to consumer privacy, including the sale or sharing of personal information, the processing of sensitive personal information, and the use of ADMT for significant decisions.

- Develop a process and format to conduct and document risk assessments for each such activity, applying the balancing test to confirm that the benefits of the processing outweigh the associated risks to consumer privacy—and, where they do not, implement appropriate modifications or safeguards to achieve that balance. Companies that have already developed a process to address the data protection impact assessment requirements under the EU and UK GDPR should try to leverage existing efforts as much as possible.

- Identify key stakeholders who will help with the preparation of the assessments themselves as well as be responsible for signing the attestations. The risk assessment process should not be siloed within a legal or compliance team. Depending on the nature of the processing activity in question, it may be necessary to involve technology, product, HR, and data engineering teams, among others. Where ADMT is involved, businesses should give particular consideration to whether it will be necessary to engage external experts as well.
- Be ready to submit the first summary of risk assessments by the April 1, 2028, deadline and every year thereafter.
- Establish processes to review and update risk assessments at least every three years or within 45 days whenever a material change to the underlying processing activity occurs.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial & Data, Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Goli Mahdavi

Global AI Lead, San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Andrea Rastelli

Associate, Boulder

andrea.rastelli@bclplaw.com

+1 303 417 8564
