JENNER & BLOCK

Client Alert: California Privacy Protection Agency Releases Initial Draft Proposed Rules for Risk Assessments and Cybersecurity Audits

Publications

September 7, 2023
By: Madeleine Findley

On August 28, 2023, the California Privacy Protection Agency ("CPPA") released an initial draft of proposed rules for privacy risk assessments and cybersecurity audits for discussion at the September 8, 2023 CPPA Board Meeting. These proposals reflect progress on long-awaited guidance from the agency on the requirements for risk assessments and cybersecurity audits required under the California Privacy Rights Act ("CPRA"). The proposals are not yet fully drafted and the CPPA has not started the formal rulemaking process. Notably, each proposal contains options for Board consideration.

The drafts nonetheless give insight into the highly detailed and prescriptive approach the agency is considering and the significant obligations it will impose on businesses, including requirements for auditors, additional requirements for processing involving artificial intelligence ("AI") or automated decisionmaking technology ("ADT"), and submission of certifications from senior business leadership. These discussion drafts offer an opportunity to identify issues for comment once the CPPA begins the formal rulemaking. The proposals are summarized below.

Proposed Draft Regulations

I. Draft Risk Assessment Regulations

The Draft Risk Assessment Regulations establish the requirements to conduct a risk assessment for businesses whose processing of personal information poses a "significant risk to consumers' privacy." The proposal is similar to guidance for data protection assessments under the Colorado Privacy Act and the GDPR but would impose numerous specific reporting and compliance requirements.

A."Significant Risk" Triggers Risk Assessment

Before beginning any processing that would present a "significant risk" to consumers' privacy, a covered business must conduct a risk assessment.[1] "Significant risks" include selling or sharing of personal information and processing sensitive personal information. The proposal includes several further "significant risks" for CPPA consideration, including using ADT to provide or deny certain services or opportunities, processing personal information of minors, workplace and education monitoring, processing personal information of consumers in publicly accessible places, or processing personal information to train AI or ADT.[2] The draft proposes definitions for AI and ADT.

B. Content of Risk Assessment

The proposal requires a risk assessment to include "at minimum" a list of between 10 and 14 elements, depending on how the CPPA chooses among draft options. For example, an assessment must provide:

- A summary of the processing that presents significant risk to consumers' privacy, and a description of how the business will collect, use, disclose, and retain personal information;
- Categories of personal information to be processed, including sensitive personal information;
- Context of the processing activity;
- Consumers' reasonable expectations regarding the purpose of the processing;
- The operational elements of the processing (including data minimization, data retention, technology used, and names or categories of service providers, contractors, or third parties); and
- Purposes of processing

Additionally, the assessment must describe the benefits and the negative impacts of the processing, including potential constitutional, discrimination, economic, physical, reputational, and psychological harms, and any safeguards the business has implemented as a result. The risk assessment must determine whether negative impacts outweigh the benefits of the processing.[3] If the assessment determines that the risks outweigh the benefits, the business may not engage in the processing.[4]

The draft also proposes additional requirements for CPPA consideration, including identification of internal and external contributors to the assessment, any internal or external audit conducted in connection with the assessment, and—in one option—a signed certification from the highest-ranking executive responsible for oversight of risk-assessment compliance that they have reviewed, understood, and approved the assessment.[5]

A business may rely on a risk assessment conducted under another similar privacy law, to the extent that assessment satisfies the requirements of the regulations. The business may supplement the prior assessment to address any gaps between regulatory frameworks.

C. Additional Requirements for Artificial Intelligence and Automated Decisionmaking Technology

Businesses that process personal information in connection with AI or ADT would be required to comply with additional detailed requirements, including providing plain language explanations of the purpose for using AI or ADT, the outputs of the processing, evaluations of AI or ADT for validity, reliability, and fairness, and any human involvement. If the business uses personal information to train AI or ADT and makes that AI or ADT available to other businesses or customers, the assessment must also explain how the business provides, to those other persons, the appropriate purposes for which the AI or ADT may be used, and safeguards it has implemented to ensure the AI or ADT is used for appropriate purposes.[6]

D. Timing & Compliance

Businesses would be required to conduct risk assessments before undertaking new processing activities, and would have 24 months to assess ongoing processing.[7] Risk assessments would have to be updated whenever there is a "material change" to the processing, and at intervals of one to three years, depending which option the CPPA selects.[8]

The proposal includes only a summary description of required compliance submissions to the agency. Proposed regulations not yet drafted would require businesses to make risk assessments available to the CPPA and the California Attorney General upon request. Businesses also would need to annually submit to the CPPA an "abridged form" of the risk assessments and a certification from a designated executive that the business has complied with the assessment requirements.[9] The content of these abridged risk assessments will likely be the subject of further drafting and significant stakeholder interest.

II. Cybersecurity Audits

The Draft Cybersecurity Audit Regulations set out the specifications for completing a required annual cybersecurity audit.

A. "Significant Risk to Consumers' Security"

Any business that processes personal information in a manner presenting "significant risk to consumers' security" would be required to conduct an annual cybersecurity audit.[10] The draft would deem data brokers to pose a "significant risk." It also presents options for CPPA consideration about other businesses or business practices that constitute a "significant risk," including businesses:

- processing personal information, sensitive personal information, or personal information of known minors above certain thresholds of consumers[11]

- with annual gross revenues above an unspecified threshold[12]
- with more than an unspecified number of employes[13]

B. Requirements of Cybersecurity Program

Any cybersecurity program would be required to contain specified elements or explain in writing why the element is not needed.[14] Among other things, the audit must describe how the business addresses 17 safeguards "to protect personal information from internal and external risks to the security, confidentiality, integrity, or availability of personal information,"[15] including (among others) authentication, encryption, account management, vulnerability scans, network monitoring and defense, cybersecurity training, oversight of service providers and third parties, retention schedules and incident response plans.[16] Additionally, the audit must identify and describe any breach notifications to regulators or consumers, and remediation measures taken.

C. Independent Auditor

The draft proposal would require businesses to use a "qualified, objective, independent" auditor.[17] An auditor can be internal but must be independent and shall report "directly to the business's board of directors or governing body, not to business management" overseeing the cybersecurity program.[18]

D. Contents of Cybersecurity Audit

The proposal would require the cybersecurity audit to (1) assess, document, and summarize each component of the business's cybersecurity program; (2) identify any gaps or weaknesses; (3) address the status of any previously identified gaps or weaknesses; and (4) identify any corrections or amendments to prior cybersecurity audits.[19] The audit should also identify the auditor and all employees responsible for the cybersecurity program.[20]

The draft proposes two options on how an audit should assess and document the business's cybersecurity program. The first would look at how the business considers and protects against six specific types of negative impact to consumer security, including security incidents, economic, physical, psychological or reputational harms.[21] The second would assess and document risks from cybersecurity threats that have or are reasonably likely to materially affect consumers.[22]

E. Timing & Compliance

Businesses would have 24 months to conduct their first cybersecurity audit, and then annually thereafter.[23] Additionally, a member of the business's Board or governing body, or its highest-ranking executive would be required to submit a written certification of compliance to the CPPA that

the business has complied with the audit requirements or, if not, that identifies which provisions have not been addressed and a remediation timeline.[24]

III. Next Steps

The CPPA will discuss the two proposals at its September 8, 2023 Board meeting. Staff will likely revise the drafts based on those discussions, and present updated drafts to start a formal rulemaking at an upcoming meeting. The next regularly scheduled CPPA Board meeting will be in November.

Footnotes

[1] *Id.*§ 7150(a).

[2] *Id.* § 7150(b)(1)–(2).

[3] *Id.* § 7152(a)(1)–(10).

[4] *Id.* § 1755.

[5] *Id.* § 7153(a)(11)–(14), Option I and II.

[6] *Id.* §§ 7153–7154.

[7] *Id.* § 7156(c).

[8] *Id.* § 7156(a)(3)(A)–(O).

[9] *Id.* § 7158

[10] Draft Cybersecurity Audit Regulations §§ 7001(i), 7120(a).

[11] *Id.* § 7120(b)(2), Option I.

[12] *Id.*, Option II.

[13] *Id.*, Option III.

[14] *Id.* § 7123(c)(1).

[15] *Id.* § 7123(c)(2).

[16] *See id.* § 7123(c)(2)(A)–(R).

[17] *Id.* § 7122(a).

[18] *Id.* § 7122(a)(2).

[19] *Id.* § 7122(e).

[20] *Id.* §§ 7122(f), 7123(c)(1)(A)(i).

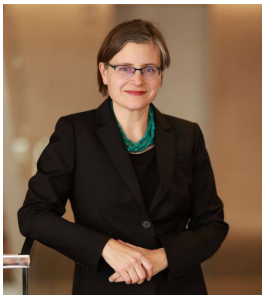
[21] *Id.* § 7123(b), Option I.

[22] *Id.*, Option II.

[23] *Id.* § 7121.

[24] *Id.* § 7124.

Related Attorneys



Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095

Related Capabilities

Data Privacy and Cybersecurity