SQUIRE PATTON BOGGS

Light at the End of the Tunnel

Are You Ready for the New California Privacy and Cybersecurity Rules?

After what seems like forever, the most recent (and last?) public comment period for the draft California Consumer Privacy Act (**CCPA**) regulations finally closed on February 19, 2025. (Read *Privacy World* coverage here and here.)

Following an initial public comment period on an earlier draft, the formal comment period for the current version of the proposed CPPA regulations (**Proposed Regulations**) began on November 22, 2024. The Proposed Regulations include amendments to the existing CCPA regulations and new regulations on automated decision-making technology, profiling, cybersecurity audits, requirements for insurance companies and data practice risk assessments. The California Privacy Protection Agency (**CPPA**) may either submit a final rulemaking package to the California Office of Administrative Law (**OAL**, which confirms statutory authority) or modify the Proposed Regulations in response to comments received during the public comment period.

If the CPPA proposes new changes to the Proposed Regulations, a new 15-day comment period follows. During the 15-day period, new comments must relate only to the CPPA's newly proposed changes. This process repeats until the CPPA submits its final rulemaking package to the OAL. The OAL has up to 30 business days to review and approve the CPPA's final rulemaking package. Once the OAL approves, the effective date of the Proposed Regulations (**Effective Date**) is determined by § 11343.4(b)(3) of the California Government Code.

We are hopeful that the CPPA and OAL will issue final regulations by this summer. Once final, some requirements apply as of the Effective Date and others phase-in for up to 24 months after the Effective Date.

This means that, even though the CPPA could further modify the Proposed Regulations, the immediate effectiveness of parts of the Proposed Regulations calls for businesses to start their preparations now.

We addressed the notable amendments to the existing CCPA regulations in a prior post. We offer a quick summary of the new requirements and compliance timing, as well as a checklist to help jump-start the compliance process below. All references to section numbers and compliance dates relate to the Proposed Regulations. (*Privacy World* will consider the requirements for insurance companies in a future post.)

For more detailed guidance on complying with the current CCPA regulations and the Proposed Regulations, Squire Patton Boggs Services Ireland, Limited, Ankura Consulting Group, LLC and Exterro, Inc. have developed assessment templates, checklists and comparison charts that are available for license as non-legal services.[1] More information is available here. Squire Patton Boggs (US) LLP offers additional guidance, customization and counsel to its legal service clients.

1 DISCLAIMER — PRIVACY POWERED BY SQUIRE PATTON BOGGS:™ (1) Provided as educational reference material and not legal advice; and (2) There is no attorney-client relationship with Squire Patton Boggs unless a written attorney-client engagement agreement is entered into with Squire Patton Boggs. Use of licensed materials is subject to the terms of the license between the end user and licensor Squire Patton Boggs Services Ireland, Limited, including limiting access and use to the licensee. Consult legal counsel with regard to use of the materials.

While every effort has been made to ensure that the information contained in this article is accurate, neither its authors nor Squire Patton Boggs accepts responsibility for any errors or omissions. The content of this article is for general information only, and is not intended to constitute or be relied upon as legal advice.

ankura exterro

Contacts

Alan Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Julia Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Glenn Brown
Principal, Atlanta
T +1 678 272 3235
E glenn.brown@squirepb.com

Lydia de la Torre
Of Counsel, Palo Alto
T +1 650 843 3227
E lydia.delatorre@squirepb.com

Sasha Kiosse
Associate, New York
T +1 212 872 9861
E sasha.kiosse@squirepb.com

What are the 2025 Proposed Regulations? How Do They Compare to Other States' Obligations?

The Proposed Regulations amend the existing regulations and add new requirements covering automated decision-making technology (**ADMT**), profiling, cybersecurity audits, requirements for insurance companies and data practice risk assessments.

Many states regulate profiling, but none has done so as robustly as the CPPA proposes. Most states have whole or partial exemptions for insurance businesses. While assessment requirements are included in most of the other state consumer privacy laws, the Proposed Regulations exceed the other states' requirements in operational and reporting requirements. The cybersecurity audit requirements in the Proposed Regulations are unique to California. Also, only California regulates personal information in business-to-business and human resources contexts, which makes the scope of the Proposed Regulations broader than in other states' consumer privacy laws.

Assessment requirements under other state consumer privacy laws include:

- **Virginia** – Assessments are required for processing activities conducted or generated after January 1, 2023.
- **Colorado, Connecticut and Florida** – Assessments are required for processing activities conducted or generated after July 1, 2023. (The Colorado consumer privacy law prescribes detailed requirements on how to conduct and document assessments.)
- **New Hampshire, Oregon, Tennessee**[2] **and Texas** – Assessments are required for processing activities created or generated after July 1, 2024.
- **Montana** – Assessments are required for processing activities that occur on or after January 1, 2025.
- **Nebraska** – Assessments are required as of the effective date of the law, January 1, 2025.
- **New Jersey** – Assessments are required for processing activities that involve personal information acquired on or after January 15, 2025.
- **Delaware** – Assessments are required for processing activities conducted or generated on or after July 1, 2025.
- **Minnesota** – Assessments are required as of the effective date of the law, July 31, 2025.
- **Maryland** – Assessments are required for processing activities that occur on or after October 1, 2025.
- **Indiana** – Assessments are required for processing activities created or generated after December 31, 2025.
- **Rhode Island** – Assessments are required for processing activities that occur on or after January 1, 2026.
- **Kentucky** – Assessments are required for processing activities created or generated on or after June 1, 2026.

Despite some material differences, the Proposed Regulations are like the assessment requirements in the Colorado Privacy Act but other state consumer privacy laws do not have as detailed assessment requirements. Businesses may wish to consider the assessment requirements in the California or Colorado consumer privacy laws – or even the European Data Protection Board guidelines under GDPR (which seem to have influenced Colorado and California) - as benchmarks.

Learn more about data privacy risk assessments here, **and** here.

When Do We Need to Comply with Which of the Proposed Regulations?

Requirements That Apply as of the Effective Date

Notice of Use of ADMT

- A business must provide a "**Pre-use Notice**" *before* the business processes a consumer's personal information:
  - (1) using ADMT for a "**significant decision**" (§ 7200(a)(1)) or for "extensive profiling" (§ 7200(a)(2)), or
  - (2) for training uses of ADMT that is capable of use (a) for a significant decision, (b) to establish individual identity, (c) for physical or biological identification or profiling, or (d) for the generation of a "deepfake." § 7220(a)(3).
- A business that uses ADMT to make certain a significant decision adverse to a consumer must provide the consumer with notice of the consumer's "**right to access ADMT**" (§ 7001(vv)) as soon as feasibly possible but no later than 15 business days after the date of the adverse significant decision. § 7222(k).

Request to Opt-Out of ADMT

- If a consumer submits a "**request to opt-out of ADMT**" *before* the business has initiated that processing, the business must not initiate the processing. § 7221(m).
- If a consumer submits a **request to opt-out of ADMT** after the business has initiated that processing, and none of the Opt-out Exceptions (defined below) apply, then the business must cease processing the consumer's personal information as soon as feasibly possible but no later than 15 business days after the date of receipt of the consumer's request (which is the same timing as the opt-out of sale/sharing). § 7221(n).
- **Opt-Out Exceptions** include security, fraud prevention, and safety; certain admission, acceptance, or hiring decisions, assignment of work and compensation decisions, educational profiling, and a method provided by the business for a consumer to appeal the ADMT decision to a qualified human reviewer who has the authority to overturn the decision (among others). § 7221(b).

Request to Access ADMT and Right to Appeal ADMT

- No later than 10 business days after receipt of either a "**request to access ADMT**" (§ 7001(vv)) or a "**request to appeal ADMT**" (§ 7001(nn)), a business must confirm receipt of the request. (The request to appeal ADMT applies only if the business is providing the human appeal right instead of the ADMT opt-out right.) § 7021(a).
- No later than 45 calendar days after receipt of the request, a business must respond to a request to access ADMT and a request to appeal ADMT, subject to a 45-calendar-day extension. § 7021(b).
- These timing requirements are the same as for requests to delete, correct and know.

Evaluation and Policy Requirements for Physical or Biological Identification or Profiling

- When a business uses "physical or biological identification or profiling" (**PBIP**) (§ 7001(gg)) for a significant decision or for extensive profiling, the business must evaluate the PBIP to ensure that the technology works as intended for the business's proposed use and does not discriminate based on protected classes. § 7201(a)(1).
- The business also must implement policies, procedures and training to ensure that the PBIP works as intended for the business's proposed use and does not discriminate based on protected classes. § 7201(a)(2).

Requirements That Phase In Up to 24 Months After The Effective Date

Cybersecurity Audits

- A business has up to 24 months *after the Effective Date* to complete its first cybersecurity audit. § 7121(a).
- A cybersecurity audit is required if a business's processing presents "significant risk to consumers' security." § 7120(b).

Risk Assessments

- For any processing activity requiring an assessment that the business initiated *prior to the Effective Date* and continues after the Effective Date, the business must conduct and document a risk assessment within 24 months after the Effective Date. § 7155(c).
- For processing activities conducted *after the Effective Date*, a business has 24 months to make its first submission of the risk assessment materials (compliance certificates and assessment summaries) to the CPPA. § 7157(a)(1).
- A risk assessment is required when a business's processing "presents significant risk to consumers' privacy" § 7150(a).

2 The Tennessee law is effective July 1, 2025, but assessment obligations are for activities commencing July 1, 2024.

The high-level checklist below is for educational purposes to help you prepare for the Proposed Regulations.

I. Automated Decision-making Technology and Other Related Processing

Consider whether the following apply if the business is engaging in ADMT or PBIP for a significant decision or extensive profiling:

- ☐ *If using ADMT (i) for a significant decision; (ii) for extensive profiling; or (iii) for training uses of ADMT that is capable of being used for a significant decision, to establish individual identity, for PBIP; or for the generation of a deepfake (§ 7200)*:
  - ☐ Provide consumers with a Pre-use Notice or a consolidated Pre-use Notice (i.e., a Pre-use Notice that addresses the use of ADMT for multiple purposes, or the use of multiple ADMTs) that meets the content requirements of § 7220(b)-(d).
  - ☐ Update the business's privacy policy to provide consumers the new right to opt-out of ADMT.
- ☐ *If using ADMT for (i) a significant decision or (ii) extensive profiling*: Update the business's privacy policy to provide consumers the notice of the right to access ADMT. If ADMT is used solely for training uses of the ADMT, then the business is not required to respond to a request to access ADMT, but the business still must comply with a consumer's request to know (per §7204.) § 7222(a).
- ☐ *If providing a right to appeal ADMT to a qualified human reviewer instead of a right to opt-out*: Update the business's privacy policy to provide consumers the right to appeal ADMT. § 7221(b)(2).
- ☐ Establish procedures to (1) confirm the business's receipt of a request to access ADMT or request to appeal ADMT within 10 business days after receipt of the request and provide information about how the business will process the request, (2) respond to a request to access or appeal ADMT within 45 calendar days, or 90 calendar days if the business properly extends its response period, and (3) provide all information required by § 7222 to consumers who request to access ADMT, which includes the purpose(s) for using ADMT, outputs of ADMT, how the business used outputs and the logic (i.e., operational details) of the ADMT.
- ☐ Ensure that the business stops processing a consumer's personal information for ADMT within 15 business days after the date that the consumer's request to opt-out is received unless an Opt-out Exception applies. (A business must always provide the right to opt-out for use of ADMT for profiling for behavioral advertising or for training uses of ADMT). § 7221(b)(6).
- ☐ Conduct the required evaluation of PBIP used for a significant decision or for extensive profiling and implement all required policies, procedures, and trainings to ensure that the PBIP works as intended for the business's proposed use and does not discriminate based on protected classes (n.b., this evaluation requirement is different from a risk assessment and is not subject to the 24 month phase-in.) § 7201.
- ☐ Conduct a full risk assessment (see Section II below) if the business uses ADMT for a significant decision or extensive profiling or processes personal information to train ADMT or AI that is "capable of being used" (a) for a significant decision, (b) to establish individual identity, (c) for PBIP, (d) for the generation of a deepfake or (e) for operation of "generative models." § 7150(b).

II. Risk Assessments

- ☐ Determine whether a risk assessment is needed because the processing of personal information "presents significant risk to consumers' privacy" (§ 7150(a) – (b)), which means:
  - ☐ "Selling" or "sharing" personal information
  - ☐ Processing sensitive personal information
  - ☐ Using ADMT for a significant decision
  - ☐ Using ADMT for extensive profiling
  - ☐ Processing personal information to train ADMT or AI for any of the following uses: for a significant decision, PBIP, generation of a deepfake, operation of "generative models," or to establish individual identity
- ☐ Conduct and document risk assessments as of the Effective Date within 24 months after the Effective Date. § 7155(c).
- ☐ Ensure that internal and external stakeholders contribute to or review the risk assessment according to their level of involvement with the data processing. § 7151(a).
- ☐ Ensure that the risk assessment meets all of the relevant content requirements set forth in § 7152, including:
  - ☐ Purpose(s) for processing consumers' personal information
  - ☐ Categories of personal information, including sensitive personal information, to be processed and other information about the quality of personal information as discussed in § 7152(a)(2)
  - ☐ Operational elements of the data processing, including the seven elements identified in § 7152(a)(3), such as the ADMT's "built-in" assumptions, limitations, parameters and other elements of the "logic"
  - ☐ Benefits of the data processing to the business, the consumer, other stakeholders and the public, as well as the negative impacts to consumers' privacy (consider the nine examples provided in § 7152(a)(5))
  - ☐ Safeguards that the business will implement to address the negative impacts to consumers' privacy, considering the four examples provided in § 7152(a)(6)(A) and specific questions related to use of ADMT in § 7152(a)(6)(B)

- [ ] Whether the business will initiate the data processing subject to the risk assessment (i.e., do the benefits outweigh the risks as mitigated by the safeguards?)
- [ ] All contributors to the risk assessment and dates of review and approval
- [ ] All additional inquiries related to processing to train ADMT or AI, as per § 7153

- [ ] Within 24 months after the Effective Date (unless an exemption applies), complete each required risk assessment ("first submission") and submit to the CPPA's website the first annual certification of conduct and abridged risk assessment (on a form to be provided by the CPPA). § 7157(b).
- [ ] Prepare to provide an unabridged version of each risk assessment due within 24 months after the Effective Date within 10 days after a request from the CPPA or California Attorney General. § 7157(d).
- [ ] Review and update each risk assessment at least once every three years or when a material change to the data processing is planned. § 7155.

III. Cybersecurity Audits

- [ ] Determine if the business's processing of personal information presents significant risk to consumers' security and complete a cybersecurity audit if the business (i) derived 50 % or more of its revenues in the preceding calendar year from selling or sharing California residents' personal information, or (ii) in the preceding calendar year, had global gross annual revenue of over US$25 million (as adjusted by the CCPA for inflation) and either (a) processed the personal information of 250,000 or more California residents or households, or (b) processed the sensitive personal information of 50,000 or more California residents. § 7120(b).
- [ ] Complete a cybersecurity audit using a qualified, objective and independent auditor within 24 months after the Effective Date and annually thereafter. § 7121, § 7122.
- [ ] Ensure that the cybersecurity audit contains the required content. § 7122(d)-(i), § 7123.
- [ ] Starting two years after the Effective Date, submit to the CPPA each calendar year a written certification that the business completed a compliant cybersecurity audit. § 7121(a), § 7124(a).

In addition to the compliance steps outlined above, meeting the consumer rights, evaluation and assessment obligations in the Proposed Regulations also will require careful diligence of, and contracting with, technology providers and processors, particularly for recruitment and employment practices that are most likely to generate significant decisions and risks, and these upcoming requirements are under the radar of many HR departments. For more information, please contact any of the authors or your Squire Patton Boggs relationship partner.