

California Privacy Protection Agency

Proposed Text: Opt-Out Preference Signals (OOPS)

California Code of Regulations

Title 11. Law

Division 6. California Privacy Protection Agency

Chapter 1. California Consumer Privacy Act Regulations

Amend the following Articles to add the blue underlined text and delete the ~~red strikethrough text~~:

Article 3. Business Practices for Handling Consumer Requests

§ 7025. Opt-out Preference Signals.

- (a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.
- (b) A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:
 - (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field, like Global Privacy Control (GPC), or JavaScript object.
 - (2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.
- (c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):
 - (1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing



for the consumer. This is not required for a business that does not sell or share personal information.

- (2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, including pseudonymous profiles.
- (3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display the status of the consumer's choice in accordance with section 7025, subsection (c)(6), and section 7026, subsection (g).
- (4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business may notify the consumer that processing the opt-out preference signal as a valid request to opt-out of sale/sharing would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the business asks and the consumer does not affirm their intent to withdraw, the business may ignore the opt-out preference signal with respect to that consumer's participation in the financial incentive program for as long as the consumer is known to the business. If the business does not ask the consumer to affirm their intent with regard to the financial incentive program, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business



associates with that browser or device. In either situation, the business must display the status of the consumer's choice in accordance with section 7025, subsection (c)(6), and section 7026, subsection (g).

- (5) Where the consumer is known to the business, the business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.
- (6) A business must display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website. For example, the business may display on its website "Opt-Out Request Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, and display through a toggle or radio button that the consumer has opted out of the sale/sharing of their personal information in accordance with section 7026, subsection (g).
- (7) Illustrative examples follow.
 - (A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-context behavioral advertising. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's information linked to Caleb's browser identifier for cross-context behavioral advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.
 - (B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise. Business O must also wait at least 12 months before



asking Noelle to opt-in to the sale or sharing of her personal information in accordance with section 7026, subsection (k). In addition, Business O's notification would not allow it to fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because it would not be complying with the requirements set forth in subsection (f).

- (C) Angela also has an account with Business O and has enabled an opt-out preference signal on her browser while logged into her account. Business O applies the opt-out preference signal as a valid request to opt-out of sale/sharing not only to Angela's current browser, but also to Angela's account because she is known to the business while making the request. Angela later logs into her account with Business O using a different device that does not have the opt-out preference signal enabled. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.
- (D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits with marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.
- (E) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device and any consumer profile the business associates with that browser or device.
- (F) Business SS allows third parties to place cookies on its website so they can track consumers' browsing activity across different sites and applications for cross-context behavioral advertising. These third parties engage in cookie syncing, meaning they match their respective user IDs to identify the same consumer across browsers or devices and enhance the consumer's ad-targeting profile. When Business SS receives an OOPS, it must not allow these third parties to initiate or perform cookie-syncing for cross-context behavioral purposes. Accordingly, Business



SS must configure its website to prevent those third parties' tracking technologies from initiating or performing cookie syncing for cross-context behavioral purposes whenever it receives a GPC signal.

- (G) Business ABC is a retailer that uses tracking technologies to recognize the same consumer across its various websites, mobile applications, and other digital platforms. When Lucy views a product on Business ABC's website on her laptop, and later visits the same website on her phone, Business ABC uses matching technologies, like fingerprinting, to link those devices and create a pseudonymous profile of her, even without her name or an account login. Business ABC uses and shares this information for cross-context behavioral advertising purposes that constitute a sale or sharing of personal information. Lucy enables GPC on the browser on her laptop and revisits Business ABC's website from that browser. Because Business ABC tracks Lucy across its different digital properties, it must stop selling and sharing personal information associated with her laptop browser as well as any other devices, such as her phone, that are linked to her pseudonymous profile.
- (H) Business CBA is a retailer that does not use tracking technologies to recognize or link the same consumer across its various websites, mobile applications, or other digital platforms. Instead, it maintains consumers' information in an unlinked, device-specific form. When Valen visits Business CBA's website from his laptop browser, the business applies the OOPS to the personal information associated with that specific device and browser. Because Business CBA does not associate any other devices or browsers with a pseudonymous profile for Valen, it is not required to extend Valen's OOPS to those other devices or browsers.

- (d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.
- (e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provide a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the Alternative Opt-out Link. They do not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out



preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g), then it may, but is not required to, provide the above-referenced links.

- (f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:
 - (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.
 - (2) Change the consumer's experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business's product or service functions compared to a consumer who does not use an opt-out preference signal.
 - (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. However, a business's display of whether the consumer visiting their website has opted out of the sale or sharing their personal information shall not be considered a violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) – (3).
- (g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the "Do Not Sell or Share My Personal Information" link or the Alternative Opt-out Link if it meets all of the following additional requirements:
 - (1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.
 - (2) Includes in its privacy policy the following information:
 - (A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;
 - (B) A statement that the business processes opt-out preference signals in a frictionless manner;
 - (C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner; and



- (D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.
- (3) Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.
 - (A) Business Q collects consumers' online browsing history and shares it with third parties for cross-context behavioral advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.
 - (B) Business R only sells and shares personal information online for cross-context behavioral advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1), and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

(h) If a browser, as defined by Civil Code section 1798.136(e)(1), has a feature, tool, or function that interacts with a business on the consumer's behalf and that feature makes the consumer's personal information available to the business, that feature must not prevent, interfere with, contradict, or disable the consumer's opt-out preference signal or other setting indicating the consumer's choice to opt-out of the sale or sharing of their personal information from being sent to the business.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7026. Requests to Opt-out of Sale/Sharing.

- (a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third



parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

- (1) A business that collects personal information from consumers online shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods: an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy if the business processes an opt-out preference signal in a frictionless manner.
 - (2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out of sale/sharing in addition to the opt-out preference signal.
 - (3) Other methods for submitting requests to opt-out of the sale/sharing include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.
 - (4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.
- (b) A business’s methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.
 - (c) A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer’s personal information.
 - (d) A business shall not require a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.
 - (e) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The



business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

- (f) A business shall comply with a request to opt-out of sale/sharing by:
- (1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors collecting personal information pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information.
 - (2) Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person to whom the third party has made the personal information available during that time period.
 - (3) Illustrative examples follow.
 - (A) Business U uses programmatic advertising technology on its website that instantaneously sells and shares personal information of consumers viewing its website through real-time bidding. Business U can restrict the transfer of personal information instantaneously, and thus, stop the sale and sharing personal information immediately. Accordingly, when Maya visits Business U's website and submits a request to opt-out of sale/sharing through the "Do Not Sell or Share My Personal Information" link, Business U shall immediately comply with Maya's request by ceasing to sell or share Maya's personal information with any third parties. Business U shall not take 15 business days to comply with Maya's request because it is feasibly possible to comply with the request sooner.
 - (B) Business V is a marketing company that discloses consumers' personal information to its clients via a batched upload every Friday. Business V's disclosure of personal information is a sale because it receives valuable consideration in exchange for the information. Siobhan submits a request to opt-out of sale/sharing to Business V through the mail, which Business V receives on Thursday. Business V finishes processing Siobhan's request on Tuesday because it requires a few days to update all internal systems and databases with Siobhan's request. Accordingly, Siobhan's personal information was not removed from the disclosure that occurred on the first Friday after receiving her request, though it was removed from the disclosure that occurred on the second Friday. Business V must notify all its clients that received Siobhan's information



on the first Friday after Siobhan made her request to opt-out of sale/sharing and direct them to comply with her request and forward the request to any other person to whom they made Siobhan's personal information available.

(C) Business WWW is an online retailer that uses a consent management platform (CMP) and a tag management system (TMS) on its website to process consumers' requests to opt out of the sale or sharing of personal information. Business WWW configures its website so that third-party advertising and analytics cookies and pixels that facilitate the sale or sharing of personal information are set before the CMP and TMS determine whether it has received the consumer's GPC signal. Violet visits Business WWW's website with GPC enabled in her browser and her request to opt out of sale and sharing is received as soon as Violet's browser sends the initial request to access the website. By configuring its website to sell and share personal information before determining whether it has received Violet's GPC signal, Business WWW has not complied with her request as soon as feasibly possible in violation of section 7026(f)(1).

- (g) A business must provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Opt-Out Request Honored" in accordance with section 7025, subsection (b)(6), and display in the consumer's privacy settings through a toggle or radio button that the consumer has opted out of the sale/sharing of their personal information.
- (h) In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing of personal information for certain uses as long as a single option to opt-out of the sale or sharing of all personal information is also offered. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).
- (i) A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).
- (j) A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and



provide written permission from the consumer does not apply to requests made by an opt-out preference signal.

- (k) Except as allowed by these regulations, a business shall wait at least 12 months from the date of the consumer's request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

Article 5. Verification of Requests

§ 7060. General Rules Regarding Verification.

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to delete, request to correct, request to know, ~~or~~ request to access ADMT, or request to appeal ADMT is the consumer about whom the business has collected information.
- (b) A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing, to make a request to limit, or to make a request to opt-out of ADMT. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license.
- (c) In determining the method by which the business will verify the consumer's identity, the business shall:
 - (1) Match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business before requesting additional information, or use a third-party identity verification service that complies with this section.
 - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.
 - (3) Consider the following factors:
 - (A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive personal information shall warrant a more stringent verification process.
 - (B) The risk of harm to the consumer posed by any unauthorized deletion, correction, or access. A greater risk of harm to the consumer by



unauthorized deletion, correction, or access shall warrant a more stringent verification process.

- (C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.
 - (D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.
 - (E) The manner in which the business interacts with the consumer.
 - (F) Available technology for verification.
- (d) A business shall avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.
- (e) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to delete, request to correct, or request to know. For example, a business must not require a consumer to provide a notarized affidavit to verify their identity unless the business pays for or compensates the consumer for the cost of notarization. A business that compensates the consumer for the cost of the notarization shall provide the consumer with instructions on how they will be reimbursed prior to the consumer's submission of the notarized affidavit.
- (f) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized deletion, correction, or access to a consumer's personal information, or access to information about a business's use of ADMT with respect to a consumer.
- (g) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.
- (h) For requests to correct, the business must verify the consumer based on personal information that is not the subject of the request to correct. For example, if the consumer is contending that the business has the wrong address for the consumer, the business shall not use address as a means of verifying the consumer's identity.



Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

Article 8. Training and Record-Keeping

§ 7102. Metrics Reporting Requirements for Businesses **Collecting Large Amounts of Personal Information.**

- (a) A business that is required to complete a cybersecurity audit under section 7120, or a risk assessment under section 7150, or knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:
- (1) Compile the following metrics for the previous calendar year:
 - (A) The number of requests to delete that the business received, complied with in whole or in part, and denied.;
 - (B) The number of requests to correct that the business received, complied with in whole or in part, and denied.;
 - (C) The number of requests to know that the business received, complied with in whole or in part, and denied.;
 - (D) The number of requests to access ADMT that the business received, complied with in whole or in part, and denied.;
 - (E) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied. Of the number of requests received, the business must separately identify the number of requests that were received from an opt-out preference signal.;
 - (F) The number of requests to limit that the business received, complied with in whole or in part, and denied.;
 - (G) The number of requests to opt-out of ADMT that the business received, complied with in whole or in part, and denied. ~~;~~ **and**
 - (H) The median or mean number of days within which the business substantively responded to requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.
 - (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. In its disclosure, a



business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

- (b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

Article 9. Cybersecurity Audits

§ 7122. Thoroughness and Independence of Cybersecurity Audits.

- (a) Every business required to complete a cybersecurity audit pursuant to this Article must do so using a qualified, objective, independent professional (“auditor”) using procedures and standards accepted in the profession of auditing, such as procedures and standards provided or adopted by the American Institute of Certified Public Accountants, the Public Company [Accounting Accountability](#) Oversight Board, the Information Systems Audit and Control Association, or the International Organization for Standardization.
 - (1) To be qualified, an auditor must have knowledge of cybersecurity and how to audit a business’s cybersecurity program.
 - (2) The auditor may be internal or external to the business but must exercise objective and impartial judgment on all issues within the scope of the cybersecurity audit, must be free to make decisions and assessments without influence by the business being audited, including the business’s owners, managers, or employees; and must not participate in activities that may compromise the auditor’s independence. For example, the auditor must not participate in business activities that the auditor may assess in the current or subsequent cybersecurity audits, including developing procedures, preparing the business’s documents, making recommendations regarding the business’s cybersecurity program (separate from articulating audit findings), or implementing or maintaining the business’s cybersecurity program.
 - (3) If a business uses an internal auditor, to maintain the auditor’s independence, the highest-ranking auditor must report directly to a member of the business’s executive management team who does not have direct responsibility for the business’s cybersecurity program. A member of the business’s executive



management team who does not have direct responsibility for the business's cybersecurity program must conduct the highest-ranking auditor's performance evaluation, if any, and determine the auditor's compensation.

- (b) The business must make available to the auditor all information in the business's possession, custody, or control that the auditor requests as relevant to the cybersecurity audit (e.g., information about the business's cybersecurity program and information system and the business's use of service providers or contractors). For example, the auditor may request information to determine the scope of the cybersecurity audit and the criteria the cybersecurity audit will use.
- (c) The business must make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit and must not misrepresent any fact relevant to the cybersecurity audit.
- (d) No finding of any cybersecurity audit may rely primarily on assertions or attestations by the business's management. Cybersecurity audit findings must rely primarily upon the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) that the auditor deems appropriate.
- (e) The cybersecurity audit report must include the information set forth in section 7123, subsection (e).
- (f) The cybersecurity audit report must be provided to a member of the business's executive management team who has direct responsibility for the business's cybersecurity program.
- (g) The business and the auditor must retain all documents relevant to each cybersecurity audit for a minimum of five (5) years after completion of the cybersecurity audit.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7124. Certification of Completion.

- (a) Each calendar year that a business is required to complete a cybersecurity audit pursuant to this Article, it must submit to the Agency a written certification that the business completed the cybersecurity audit as required by this Article.
- (b) The business must submit the certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.
- (c) The written certification must be completed by a member of the business's executive management team who:
 - (1) Is directly responsible for the business's cybersecurity-audit compliance;



- (2) Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and
- (3) Has the authority to submit the business's certification to the Agency.
- (d) The written certification must be completed and submitted to the Agency via its website at <https://cppa.ca.gov/>. The certification must include:
 - (1) The business's name and point of contact for the business, including the contact's name, phone number, and email address.
 - (2) A statement that the business has completed the cybersecurity audit.
 - (3) The time period covered by the cybersecurity audit, by month and year.
 - (4) ~~An electronically~~ signed attestation to the following statement: "I attest that I meet the requirements of California Code of Regulations, Title 11, section 7124, subsection (c), to submit this certification. Under penalty of perjury under the laws of the state of California, I hereby declare that to the best of my knowledge the information contained within and submitted with this certification is true and correct and that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit."
 - (5) The name and business title of the person submitting the certification, and the date of the certification.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

Article 10. Risk Assessments

§ 7157. Submission of Risk Assessments to the Agency.

- (a) Timing of Risk Assessment Submissions.
 - (1) For risk assessments conducted in 2026 and 2027, the business must submit to the Agency the information required by subsection (b) no later than April 1, 2028.
 - (2) For risk assessments conducted after 2027, the business must submit to the Agency the information required by subsection (b) no later than April 1 following any year during which the business conducted the risk assessments. For example, for risk assessments conducted in 2028, the business must submit to the Agency the information required by subsection (b) no later than April 1, 2029.
- (b) A business must submit to the Agency the following risk assessment information:



- (1) The business's name and a point of contact for the business, including the contact's name, phone number, and email address.
 - (2) The time period covered by the submission, by month and year.
 - (3) The number of risk assessments conducted or updated by the business during the time period covered by the submission, in total and for each of the processing activities identified in section 7150, subsection (b).
 - (4) Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of each of the categories of personal information and sensitive personal information identified in Civil Code section 1798.140, subdivisions (v)(1)(A)-(L), (ae)(1)(A)-(G), and (ae)(2)(A)-(C).
 - (5) A signed attestation to the following statement: "I attest that the business has conducted a risk assessment for the processing activities set forth in California Code of Regulations, Title 11, section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). Under penalty of perjury under the laws of the state of California, I hereby declare that to the best of my knowledge the risk assessment information submitted is true and correct."
 - (6) The name and business title of the person submitting the risk assessment information, and the date of the certification.
- (c) The individual submitting the information set forth in subsection (b) must be a member of the business's executive management team who:
- (1) Is directly responsible for the business's risk-assessment compliance;
 - (2) Has sufficient knowledge of the business's risk assessment to provide accurate information; and
 - (3) Has the authority to submit the risk assessment information to the Agency.
- (d) The risk assessment information must be submitted to the Agency via the Agency's website at <https://cppa.ca.gov/>.
- (e) The Agency or the Attorney General may require a business to submit its risk assessment reports to the Agency or to the Attorney General at any time. A business must submit its risk assessment reports within 30 calendar days of the Agency's or the Attorney General's request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.



Article 11. Automated Decisionmaking Technology

§ 7221. Requests to Opt-Out of ADMT.

- (a) A business must provide consumers with the ability to opt-out of the use of ADMT to make a significant decision concerning the consumer, except as set forth in subsection (b).
- (b) A business is not required to provide consumers with the ability to opt-out of a business's use of ADMT to make a significant decision in the following circumstances:
 - (1) The business provides the consumer with a method to appeal the decision to a human reviewer who has the authority to overturn the decision. To qualify for this exception, the business must do the following:
 - (A) Designate a human reviewer to review and analyze the output of the ADMT and any other information that is relevant to change the significant decision at issue. This human reviewer must consider the information provided by the consumer in support of their appeal and may consider any other sources of information about the significant decision. The human reviewer must know how to interpret and use the output of the ADMT that made the significant decision being appealed and must have the authority to change the decision based on their analysis.
 - (B) Clearly describe to the consumer how to submit an appeal and enable the consumer to provide information to the human reviewer in support of their appeal. The method of appeal must be easy for the consumers to execute, require minimal steps, and comply with section 7004. Disclosures and communications with consumers concerning the appeal must comply with section 7003, subsections (a)–(b). The timeline for requests to appeal ADMT must comply with section 7021. Businesses must comply with the verification requirements set forth in Article 5 when a consumer submits an appeal.
 - (2) For admission, acceptance, or hiring decisions as set forth in section 7001, subsections (ddd)(3)(A) and (ddd)(4)(A), if the following are true:
 - (A) The business uses the ADMT solely for the business's assessment of the consumer's ~~ability to perform~~[ance](#) at work or [performance](#) in an educational program to determine whether to admit, accept, or hire them; and
 - (B) The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.
 - (3) For allocation/assignment of work and compensation decisions as set forth in section 7001, subsection (ddd)(4)(B), if the following are true:



- (A) The business uses the ADMT solely for the business's allocation/assignment of work or compensation; and
 - (B) The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.
- (c) A business that uses ADMT as set forth in subsection (a) must provide two or more designated methods for submitting requests to opt-out of ADMT. A business must consider the methods by which it interacts with consumers, the manner in which the business uses the ADMT, and the ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of the business's use of the ADMT. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. Illustrative examples and requirements follow.
 - (1) A business that interacts with consumers online must, at a minimum, allow consumers to submit requests to opt-out through an interactive form accessible via an opt-out link that is provided in the Pre-use Notice. The link title must state what the consumer is opting out of, such as "Opt-out of Automated Decisionmaking Technology."
 - (2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out in addition to the online form.
 - (3) Other methods for submitting requests to opt-out include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.
 - (4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of the business's use of ADMT because cookies concern the collection of personal information and not necessarily the use of ADMT. An acceptable method for submitting requests to opt-out must be specific to the right to opt-out of the business's use of the ADMT.
- (d) A business's methods for submitting requests to opt-out of ADMT must be easy for consumers to execute, must require minimal steps, and must comply with section 7004.
- (e) A business must not require a consumer submitting a request to opt-out of ADMT to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer.
- (f) A business must not require a verifiable consumer request for a request to opt-out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of ADMT.



However, to the extent that the business can comply with a request to opt-out of ADMT without additional information, it must do so.

- (g) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of ADMT is fraudulent, the business may deny the request. The business must inform the requestor that it will not comply with the request and must provide to the requestor an explanation why it believes the request is fraudulent.
- (h) A business must provide a means by which the consumer can confirm that the business has processed their request to opt-out of ADMT.
- (i) In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of ADMT as long as the business also offers a single option to opt-out of all of the business's uses of ADMT set forth in subsection (a).
- (j) A consumer may use an authorized agent to submit a request to opt-out of ADMT as set forth in subsection (a) on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.
- (k) Except as allowed by these regulations, a business must wait at least 12 months from the date the business receives the consumer's request to opt-out of ADMT before asking a consumer who has exercised their right to opt-out of ADMT, to consent to the business's use of the ADMT for which the consumer previously opted out.
- (l) A business must not retaliate against a consumer because the consumer exercised their opt-out right as set forth in Civil Code section 1798.125 and Article 7.
- (m) If the consumer submits a request to opt-out of ADMT before the business has initiated that processing, the business must not initiate processing of the consumer's personal information using that ADMT.
- (n) If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out of ADMT after the business initiated the processing, the business must comply with the consumer's opt-out request by:
 - (1) Ceasing to process the consumer's personal information using that ADMT as soon as feasibly possible, but no later than 15 business days from the date the business receives the request; and
 - (2) Notifying all the business's service providers, contractors, or other persons to whom the business has disclosed or made personal information available to process the consumer's personal information using that ADMT, that the



consumer has made a request to opt-out of that ADMT and instructing them to comply with the consumer's request to opt-out of that ADMT within the same time frame.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

§ 7222. Requests to Access ADMT.

- (a) A business that uses ADMT to make a significant decision must provide a consumer with information about this use when responding to a consumer's request to access ADMT.
- (b) When responding to a consumer's request to access ADMT, a business must provide plain language explanations of the following information to the consumer:
 - (1) The specific purpose for which the business used ADMT with respect to the consumer. The business must not describe the purpose in generic terms, such as "to make a significant decision ~~improve our services~~."
 - (2) Information about the logic of the ADMT. Such information must enable a consumer to understand how the ADMT processed their personal information to generate an output with respect to them, which may include the parameters that generated the output as well as the specific output with respect to the consumer.
 - (3) The outcome of the decisionmaking process for the consumer, including how the business used the output of the ADMT to make a significant decision with respect to the consumer. For example, this may include information about whether the output was the sole factor to make the decision; and if it was not the sole factor, which other factors played a role in making the decision; and to the extent that a human was part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role was in the decisionmaking process.
 - (A) If the business also plans to use the output to make an additional significant decision concerning the consumer in the future, the business's explanation must include how the business plans to use that output to make a significant decision about the consumer in the future. For example, this may include whether the output will be the sole factor in the decisionmaking process or what the other factors will be in that decisionmaking process; and to the extent that a human will be part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role will be in the decisionmaking process.



- (4) That the business is prohibited from retaliating against consumers for exercising their CCPA rights, and instructions for how the consumer can exercise their other CCPA rights. These instructions must include any links to an online request form or portal for making such a request, if offered by the business.
 - (A) The business may comply with the instructions requirement by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains these instructions. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain these instructions, so that the consumer is required to scroll through other information in order to find the instructions, does not satisfy the instructions requirement.
- (c) In providing the information required by subsections (b)(2)–(3), a business's response to a consumer's request to access ADMT is not required to include:
 - (1) Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or
 - (2) Information that would compromise the business's ability to:
 - (A) Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;
 - (B) Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or
 - (C) Ensure the physical safety of natural persons.
- (d) A business's methods for consumers to submit requests to access ADMT must be easy to use and must not use dark patterns. A business may use its existing methods to submit requests to know, delete, or correct as set forth in section 7020 for requests to access ADMT.
- (e) A business must comply with the verification requirements set forth in Article 5 for requests to access ADMT. If a business cannot verify the identity of the person making the request to access ADMT, the business must inform the requestor that it cannot verify their identity.
- (f) If a business denies a consumer's verified request to exercise their right to access ADMT, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business must inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer.



- (g) A business must use reasonable security measures when transmitting the requested information to the consumer.
- (h) If a business maintains a password-protected account with the consumer, it may comply with a request to access ADMT by using a secure self-service portal for consumers to access, view, and receive a portable copy of their requested information if the portal fully discloses the requested information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.
- (i) A service provider or contractor must provide assistance to the business in responding to a verifiable consumer request to access ADMT, including by providing the business with the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.
- (j) A business that used an ADMT with respect to a consumer more than four times within a 12-month period may provide an aggregate-level response to the consumer's request to access ADMT. Specifically, for the information required by subsection (b)(2), the business may provide a summary of the outputs with respect to the consumer over the preceding 12 months; the parameters that, on average over the preceding 12 months, affected the outputs with respect to the consumer; and a summary of how those parameters applied to the consumer.
- (k) A business must not retaliate against a consumer because the consumer exercised their right to access ADMT as set forth in Civil Code section 1798.125 and Article 7.
- (l) Nothing in this section prohibits a business from providing additional information to enable a consumer to understand how the ADMT was used to make a significant decision with respect to them. For example, a business may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers, such as the five most common outputs of the ADMT and the percentage of consumers that received each of those outputs during the preceding calendar year.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

