# ATTORNEY GENERAL'S PROPOSED REGULATIONS UNDER THE CCPA: WHAT YOU NEED TO KNOW

OneTrust DataGuidance Research



OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

# ATTORNEY GENERAL'S PROPOSED REGULATIONS UNDER THE CCPA: WHAT YOU NEED TO KNOW

## What has happened?

The California Attorney General ('AG'), Xavier Becerra, issued, on 10 October 2019, proposed regulations under the California Consumer Privacy Act of 2018 ('CCPA') for public consultation ('the Proposed Regulations').

In particular, the Proposed Regulations provide specific guidance with regard to the practical implementation of the CCPA and address issues, such as notices that must be provided by businesses to consumers, consumer requests to businesses, verification of such requests, business practices regarding the personal information of minors, and businesses' offering of financial incentives.

### General provisions

Article 1 of the Proposed Regulations includes certain definitions that provide clarity for terms used in the CCPA, such as:

- **household**, defined as 'a person or group of people occupying a single dwelling';
- **categories of third parties**, defined as 'types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers';
- **privacy policy**, defined as 'the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their own personal information';
- **financial incentive** defined as 'a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information'; and
- **third-party identity verification service**, defined as 'a security process offered by an independent third party who verifies the identity of the consumer making a request to the business'.

**Notice to consumers**

The Proposed Regulations explain in detail the **procedures** that must be followed when businesses provide specific notices to consumers, in particular:

- notice at collection of personal information;
- notice of right to opt-out of sale of personal information;
- notice of financial incentive; and
- privacy policy.

All notices must be presented in an **easily readable** (including in smaller screens, if applicable) and **understandable format** and, in addition, use **plain straightforward language** and **avoid technical or legal jargon**, **be available in languages** in which the business in its ordinary course provides contracts, disclaimers, sale announcement and other information and be accessible to consumers with disabilities.

The Proposed Regulations provide that a business should not use a consumer's personal information for any purpose other than those disclosed in the notice at collection, neither should it collect categories of personal information other than those disclosed in the notice at collection.

**Certain information must be provided** to the consumer at collection, including a list of the personal information to be collected, the business or commercial purposes for which each category of personal information will be used, a link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" if a business sells personal information, or in the case of offline notices, the web address for the webpage to which it links and a link to the business's privacy policy or the web address of the business's privacy policy in the case of offline notices.

Businesses which **do not** collect information directly from consumers are not obliged to provide notices at collection to the consumer, however, before the sale of such information, they must either contact the consumer directly with regard to the sale of information and provide the right to opt-out or contact the information source to confirm the provision of notice at collection and obtain signed attestations describing how notice was collected, including an example of the notice.

In addition, the Proposed Regulation stipulate that businesses that sell personal information of consumers shall provide a notice of **right to opt-out** by posting a notice on their webpage to which a consumer is directed after clicking on the "Do

Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or the download or landing page of a mobile application. Businesses that substantially interact with consumers offline are also required to notify consumers by an offline method that facilitates awareness of the consumers' right to opt-out. The notice must include a description of the opt-out right, the webform which can be used to submit the request, instructions for any other method by which requests may be submitted by a consumer, any proof required when a consumer uses an authorized agent to exercise their opt-out right and a link or the URL to the privacy policy of the business, or , or in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy. Finally, businesses are exempted from providing an opt-out right notice if they do not or will not sell personal information and they state that in their privacy policy.

A **financial incentive notice** must include succinct summary of the financial incentive or price or service difference offered, a description of the material terms of the financial incentive, the procedure that can be followed to opt-in to the financial incentive, a notification on the consumer's right to withdraw from the financial incentive, and an explanation of why the financial incentive or price or service difference is permitted under the CCPA.

According to the Proposed Regulations, **privacy policies** provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. At a minimum, a privacy policy **must make reference** to the right to know about personal information collected, disclosed, or sold, the right to request deletion of personal information, the right to opt-out of the sale of personal information, the right to non-discrimination for the exercise of a consumer's privacy rights, the authorized agent, how the business may be contacted for further information, the date the privacy policy was last updated and, if subject to record keeping requirements, the information compiled in section 999.317(g)(1) or a link to it.

**Handling consumer requests**

The Proposed Regulations provide details on the methods for submitting requests to know and requests to delete, how to respond to such requests, service providers, requests to opt-out, requests to opt-in after opting out of the sale of personal information, training and record keeping, and requests to access or delete household information.

Businesses are required to include two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's website or mobile application, including also methods such as a designated email address, a form submitted in person, and a form submitted through the mail. For right to delete requests, two or more designated methods for submitting requests to delete are required, and acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail. A two-step process is stipulated for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

When a business receives a request to know or delete, it shall **confirm receipt of request within 10 days** and provide information on how it will process the request which must describe the verification process and when the consumer should expect a response, with the exception of instances where the business has already granted or denied the request.

**Requests must be responded within a 45-day period**, which begins on the date the request was received, regardless of time required to verify the request. Provided that the business notifies the consumer and explains the reason, the business may take up to an additional 45 days to respond to a request, for a maximum total of 90 days from the day the request was received.

The Proposed Regulations provide that a person or entity shall be deemed a service provider to the extent that a person or entity provides services to a person or organization that is not a business or to the extent that a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and would otherwise meet all other requirements of a service provider under the CCPA. In addition, service providers that are businesses must comply with the CCPA and the Proposed Regulations regarding any personal information that they collect, maintain, or sell outside of their role as service providers.

For requests to opt-out, businesses shall provide **two or more designated methods for submitting requests to opt-out**, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's website or mobile application. Browser plugins or privacy settings or any other mechanism, that

communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be treated as a valid request for that browser or device, or, if known, for the consumer. As long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices, it is possible for a business to present the consumer with the choice to opt-out of sales of certain categories of personal information. Upon receiving a request to opt-out, a business shall act upon it as soon as feasibly possible, but no later than 15 days from the date the request was received whilst it shall also notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information.

Businesses are required to inform all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA and maintain records of consumer requests related to the CCPA and how the business has responded for at least 24 months. If a business alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, it must compile certain metrics for the previous calendar year, disclose such metrics within its privacy policy or posted on its website and accessible from a link included in its privacy policy and establish, document, and comply with a training policy to ensure individuals handling consumer requests are informed of CCPA requirements.

For requests submitted jointly by consumers of a household, if the business can individually verify all the members of the household subject to verification requirements, then it shall comply with the request.

### Verification of requests

Businesses must **establish, document and comply** with a reasonable method for verifying that a request has been submitted by the consumer about whom the business has collected information. Such determination method must match the identifying information provided by the consumer to the information already maintained by the business, or use a third-party identity verification service, avoid collecting personal information unless necessary, and consider factors such as type, sensitivity and value of personal information and the likelihood that fraudulent or malicious actors would seek the personal information.

Consumers with a **verified password-protected account** may be verified through the business's existing authentication practices for the consumer's account whilst, if fraudulent or malicious activity on or from the password-protected account us suspected, a business shall not comply with the request until further verification procedures determine that the consumer request is authentic.

For **requests that are submitted through authorized agents**, businesses may require that the consumer provide the written permission to do so and verify their own identity directly with the business. Such requirement does not apply when a consumer has provided the authorized agent with power of attorney.

**Special rules regarding minors**

The Proposed Regulations **create rules for minors** under 13 years of age, minors 13 to 16 years of age, and notices to such minors.

If a business knows that it collects or maintains the personal information of children **under the age of 13,** it shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. Provided methods for such consent include, a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan, the use of a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder, in connection with a monetary transaction, and the connection to trained personnel via video-conference, among others.

For **minors 13 to 16 years of age**, businesses must establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information. The business shall inform the minor of the right to opt-out at a later date and of the process for doing, when it receives a request to opt-in to the sale of information. Finally, businesses that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information of such minors without their affirmative authorization, or the affirmative authorization of their parent or guardian for minors under 13 years of age, is not required to provide the notice of right to opt-out.

**Non-discrimination**

A financial incentive or a price or service difference is considered **discriminatory** and therefore prohibited, when a business treats a consumer differently because the consumer exercised a right conferred by the CCPA or the Proposed Regulations. However, a business can offer a price or service difference it is reasonably related to the value of the consumer's data. Such value may be calculated by using factors such as the marginal or average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data, the revenue generated by the business from sale, collection, or retention of consumers' personal information and profit generated by the business from sale, collection, or retention of consumers' personal information, among other things.

**What's next?**

Any interested parties may participate in the four public hearings hosted by the AG and will be able to submit comments to the Office of the AG **on or before 5:00 P.M. Pacific Time on 6 December 2019**.

The public hearings will take place in Sacramento on 2 December 2019, in Los Angeles on 3 December 2019, in San Francisco on 4 December 2019, and in Fresno on 5 December 2019.

## HOW ONETRUST HELPS

With OneTrust, your organisation can take a holistic approach to CCPA compliance by leveraging a comprehensive suite of tools, each offering CCPA-specific functionality. By leveraging internal governance tools as well as consumer-facing tools, your organisation can pinpoint where personal data resides and how it is used; streamline your ability to act when consumers exercise their rights to information and deletion; and manage opt outs relating to the sale of personal information. The OneTrust platform directly addresses CCPA requirements and sets organisations on the right trajectory for supporting a global privacy program.

### CCPA Research & Readiness

#### OneTrust DataGuidance™

Use OneTrust DataGuidance™ to access a centralised resource aggregator that includes the full CCPA text, as well as summaries, comprehensive guides, and regulatory guidance. OneTrust DataGuidance™ is continually updated by the OneTrust global research team and includes latest amendments, news, and guidance.

#### Global Readiness & Accountability Tool

With the OneTrust Readiness & Accountability tool, leverage a research-backed CCPA readiness questionnaire, which helps assess your organisation's CCPA gaps and offers remediation recommendations to minimise risks.

### CCPA "Do Not Sell" & "Consumer Rights"

#### Consumer Rights Management

The CCPA stipulates a 45-day response timeline for consumer data requests. With OneTrust, intake consumer rights requests and leverage CCPA-specific response workflows to help your organisation respond to requests appropriately, and with built-in exception handling, reduce unnecessary work.

#### Cookie Consent & Website Scanning

OneTrust offers default cookie banners that reflect CCPA-specific messaging. Using geolocation, OneTrust can display different cookie banners with different consent models depending on the website visitor's location.

## CCPA Privacy Governance

### Data Inventory & Mapping

CCPA-specific data elements built into OneTrust help your organisation track key attributes when mapping data for CCPA compliance. Additionally, leverage bulk importing capabilities to attach CCPA-specific data elements to existing data.

### Assessment Automation

OneTrust Assessment Automation offers updated, CCPA-specific PIAs to adhere to data minimization and purpose limitation considerations outlined under the CCPA. With Assessment Automation, take advantage of automated CCPA-specific risk flagging and research-backed remediation recommendations.

### Vendor Risk Management

Leverage OneTrust Vendor Risk Management to communicate with third-party vendors to meet consumer requests for data access and deletion. Additionally, generate visuals to map vendors and data flows state by state and around the world.

### Incident & Breach Response

OneTrust Incident & Breach Response enables your organisation to analyse incidents with a built-in, California Data Breach Notification assessment template. With customisable workflows, streamline response and quickly remedy a violation within the CCPA's 30-day cure period.

## CCPA Consumer Engagement

### Consent & Preference Management

OneTrust Universal Consent & Preference Management solution helps businesses maintain records of consent. Via OneTrust, offer a preference management centre and embed a link to enable consumers to opt out of the sale of their personal information and take more control over their settings