AG's Modified Proposed Regulations under the CCPA: What You Need To Know

OneTrust DataGuidance Research

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

What has happened?

The California Attorney General ('AG'), Xavier Becerra, released, on 7 February 2020, a modified text of the proposed regulations ('the modified Proposed Regulations') under the California Consumer Privacy Act of 2018 ('CCPA') for public comment, further to the Proposed Regulations' first release in October 2019.

Definitions

The modified Proposed Regulations include new definitions for certain terms and also amend the majority of the definitions that already existed in the original text. For example, the following definitions have been introduced now, including:

- **employment benefits,** defined as 'retirement, health, and other benefit programs, services, or products to which consumers or their beneficiaries receive access through the consumer's employer';
- **employment-related information**, defined as 'personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose';
- **signed,** meaning 'that the written attestation, declaration, or permission has either been physically signed or provided electronically per the Uniform Electronic Transactions Act, Civil Code section 1633.7 et seq'; and
- **value of the consumer's data**, defined as 'the value provided to the business by the consumer's data as calculated under section 999.337.'

In addition, the following definitions have been amended significantly to provide further clarity to terms already used in the CCPA:

- **categories of third parties,** defined as 'types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers';
- **household,** defined as 'a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier';
- **price or service difference,** defined as 'any difference in the price or rate charged for any goods or services to any consumer related to the disclosure, deletion, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the disclosure, deletion, or sale of personal information, including the denial of goods or services to the consumer'; and

- **verify,** defined as 'to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or is the parent or legal guardian of that consumer who is less than 13 years of age.'

Furthermore, the modified Proposed Regulations clarify that **in order for information to be considered personal**, it will depend on whether it is maintained by a business in a manner that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. To supplement this provision, an example is provided where an IP address would not be considered personal information if it is collected by a business but is neither linked to any particular consumer or household, nor could it reasonably be linked with a particular consumer or household.

Consumer notices

A novelty of the modified Proposed Regulations is that they provide a general overview of the required notices businesses must disclose to consumers, which include:

- a privacy policy, for any business that must comply with the CCPA;
- a notice at the collection of information, for any business that collects information from a consumer;
- a notice of right to opt-out, for a business that sells personal information; and
- a notice of financial incentive for a business that offers a financial incentive or price or service difference.

With regard to the **notice at collection of personal information**, the modified Proposed Regulations provide that it must be readily available for consumers to encounter it at or before the point of collection of personal information and also introduces two new examples:

- where businesses collect personal information through a mobile app, they may link to the notice on the app's download page and within the app, such as through its settings menu; and
- where information is collected by a business over the telephone or in person, notice may be given orally.

It is also further clarified that personal information may not be used by a business for a purpose that is **materially different** than those disclosed in the notice at collection.

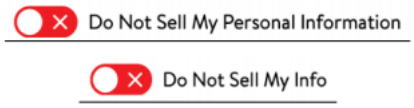
An important distinction is made for entities that are registered as **data brokers** with the AG, whereby it is provided that data brokers do not need to provide a notice to the consumer at the collection of personal information, if they have included, in their registration submission, a link to the online privacy policy with instructions on how an opt-out request may be submitted by a consumer.

Another provision introduced by the modified Proposed Regulations reflects on **employment-related information** collected by businesses: in general such businesses would still have to comply with the provisions on notice at collection, however they are exempted from including a link or a web address to a link titled 'Do Not Sell My Personal Information' or 'Do Not Sell My Info' and including a link to, or paper copy of, a business's privacy policies for job applicants, employees, or contractors in lieu of a link or web address to the business's

privacy policy for consumers. Similar to Section 1798.145, subdivision (h) of the CCPA, this provision will become inoperative on 1 January 2021, unless the CCPA is amended otherwise.

The provisions regarding the notice of the right to opt-out of sale of personal information have remained, for the most part, the same, however, the biggest novelty here is the introduction of the opt-out button, which may be used additional to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.

In addition, the modified Proposed Regulations provide that when this button is used, it must be placed to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link and must be approximately the same size as other buttons on the business's webpage.



For notices of financial incentives, the modified Proposed Regulations clarify that the purpose of the notice is to explain the **material terms** of the financial incentive or price or service difference, whilst it is also made clear that **businesses are not required to provide a notice** of financial incentive if they do not offer such an incentive or price or service difference related to the disclosure, deletion, or sale of personal information.

Additional obligations are introduced, requiring businesses to include the **value of the consumer's data** in their notice of financial incentive as well as an explanation of **how the financial incentive is reasonably related to the value of the consumer's data.**

The requirements of what should be included in a privacy policy largely remain the same, with a few further clarifications:

- on the right to know about personal information collected, disclosed or sold, businesses must identify the categories of personal information they have collected about consumers in the preceding 12 months as well as the categories of personal information that they have disclosed for a business purpose, or sold to third parties in the preceding 12 months; and
- on the right to opt-out of the sale of information, businesses must state whether or not they sell personal information, and if they do, they must include either the contents of the notice of right to opt-out or a link to it.

The modified Proposed Regulations provide that all above notices must be reasonably accessible to consumers with disabilities, and for online notices, they refer to the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium as the generally recognised industry standards.

Handling consumer requests

For the purpose of submitting **requests to know and to delete**, the modified Proposed Regulations distinguish between **businesses that operate exclusively online and have a direct relationship with a consumer from whom they collect personal information** which are only required to **provide an email address** for submitting requests to know whilst **all others** must provide **two or more methods for submitting requests**, including at least a toll-free telephone number.

Furthermore, in cases where the interaction of a business with the consumer occurs **in person,** then the business must consider providing **an in-person method**, such as a printed form that can be directly submitted or sent by mail, a tablet or computer portal or a telephone. In addition, it is no longer required that businesses use a two-step process for online requests to delete.

Regarding responses to **requests to know and to delete,** it is clarified that the confirmation of the receipt of the request must be given within **10 business days**, in the same manner in which the request was received. However, responses to such requests must be given within **45 calendar days**, whilst, if the consumer cannot be verified within the 45-day period, the business may deny the request. It is also clarified that the additional 45-day period that a business might need to respond to request refers to calendar days.

Furthermore, for responding to requests to know, the modified Proposed Regulations prescribe that businesses are not required to search for personal information if the following conditions apply cumulatively:

- personal information is not maintained by the business in a searchable or reasonably accessible format;
- personal information is maintained solely for legal or compliance purposes;
- the business does not sell personal information or uses it for any commercial purpose; and
- a description is provided to the consumer, of the categories of records that may contain personal information that were not searched because the conditions stated above were met.

Unique biometric data generated from measurements or technical analysis of human characteristics has been added to the list of information that a business is not allowed to disclose in response to a request to know.

For **responses to verified requests to know**, a business is additionally required to include the categories of personal information it has collected about the consumer in the preceding 12 months, the business purpose for which it collected or sold the personal info, the categories of third parties with which it shares personal information, as well as the categories of personal information and, for each category identified, the categories of third parties to which it sold or disclosed that particular category of information, in the preceding 12 months.

For **responses to deletion requests**, when a business sells personal information and the consumer has not requested to opt out of the sale, then the business must ask the consumer whether they would like to exercise

that right, including either the contents of, or a link to, the notice of the opt out right. A business must also inform the consumers whether or not it has complied with a deletion request and if it has indeed complied, it must inform the consumer that it will maintain a record of the request, for the purpose of ensuring that the personal information remains deleted from their records.

The provisions on service providers have been slightly amended by the modified Proposed Regulations, mainly with regard to retaining, using or disclosing of personal information in the course of providing services, which is not allowed, with the exception of:

- performance of services specified in the written contract with the business that provided the personal information;
- retaining and employing another service provider as subcontractor, who meets the CCPA requirements of a service provider;
- internal use by the service provider to build or improve the quality of its services;
- detection of data security incidents, or protection against fraudulent or illegal activity; or
- for compliance with federal, state, or local laws, or with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities, cooperation with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law, or exercise or defence of legal claims.

Service providers are also prohibited from selling data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business. In the case that service providers receive a request to know or to delete, they must either respond on behalf of the business or inform the consumer that the request cannot be acted upon due to the request having been sent to a service provider.

Specifically for opt-out requests, the modified Proposed Regulations add that the methods of submission must be easy for consumers to execute and must require minimal steps to allow opting out. They also prohibit the utilisation of methods designed to subvert or impair a decision from the consumer to opt-out.

In cases where information is collected online, via for example a browser plugin or privacy setting, that may be used to communicate the consumer's choice to opt-out, such privacy control must clearly communicate the intention to opt-out and require the consumer **affirmatively** select their choice to opt-out and must not be designed with any pre-selected setting. If such control is in conflict with an existing business-specific privacy setting of a consumer, then the business must respect the control but may notify the consumer and give them the option to confirm the privacy setting or participate in the financial incentive programme.

Businesses have 15 business days to comply with a request to opt-out from the date the request was received. For cases where personal information has been sold to any third parties after the submission of the request and before the business complies with the request, it must notify those third parties of the opt-out request and direct them to not sell that personal information.

For requests to **opt-in after opting out of the sale of information**, where a consumer who has opted out, initiates a transaction or attempts to use a product or service that requires sale of personal information, a business may provide that information along with instructions on how the consumer can opt in.

Record-keeping requirements have been enhanced with provisions on implementing and maintaining reasonable security procedures and practices in maintaining the consumer requests records and, additionally, on introducing an exception to using information for record-keeping purposes to review and modify the processes for compliance with the CCPA. Such information may not be shared with any third party.

The obligation for businesses that process the information of 10,000,000 or more consumers to compile certain metrics in a calendar year, has been clarified that it must be disclosed by July 1 of every calendar year, within the privacy policy or posted on the business's website. This disclosure may identify the number of requests denied in whole or in part by the business because the request was not made by a consumer, called for information exempt from disclosure or was denied on other grounds.

The provisions on requests to access or delete household information have been amended with regard to non-password protected accounts, where businesses shall not comply, unless:

- all consumers of the household jointly request specific pieces of information or the deletion of household personal information;
- all members are verified by the business individually; and
- the business verifies that each member making the request is currently a member of the household.

For password-protected accounts, requests relating to household information may be processed through the business's existing practices. For minors under 13, verifiable parental consent must be obtained.

Verification of requests

The modified Proposed Regulations stipulate that a consumer cannot be required to pay a fee for the verification of their request to know or to delete. In addition, they outline two examples for verification of non-account holders and also provide that a business can deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor. For verification of any requests, if there is no reasonable method by which a consumer may be verified, the business must explain why it has no reasonable verification method in its privacy policy.

Rules regarding minors

For the consent form that may be signed by the parent or a guardian of a child, it is clarified that this can be done either physically or electronically and, in addition, a requirement is created to establish, document, and comply with a reasonable method, for determining whether a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.

Non-discrimination

The modified Proposed Regulations provide that a business should not offer financial incentives, or price or service difference if it is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to that value. Also, denying a consumer request for reasons permitted by the CCPA or the Regulations must not be considered discriminatory. Finally, in order to calculate the value of consumer data, businesses can consider the value of data of all natural persons to the business and not just consumers.

What's next

The California Department of Justice is accepting written comments regarding the modified Proposed Regulations until 5:00 p.m. on 25 February 2020 by email to PrivacyRegulations@doj.ca.gov, or by mail at the following address:

Lisa B. Kim, Privacy Regulations Coordinator

California Office of the Attorney General

300 South Spring Street, First Floor

Los Angeles, CA 90013

Email: PrivacyRegulations@doj.ca.gov