PILLAR LEGAL

CCPA – "California's GDPR" Finalized Just Before July 1, 2020 Enforcement Date

U.S. TECH LAW UPDATE[1]

July 9, 2020

By: Greg Pilarowski | Alexandra Ashbrook

I. Introduction

Almost a full two years after the California Consumer Protection Act ("CCPA" or the "Act") was signed into law, California begins its enforcement of the CCPA on July 1, 2020.[2] The CCPA, which came into effect in the beginning of 2020, is one of a few robust state data privacy laws passed in the wake of Europe's implementation of the General Data Protection Regulation ("GDPR"). Section III of this U.S. Tech Law Update provides a comparative view of the GDPR and California's finalized CCPA.

The original Act, signed by then California governor Jerry Brown, faced criticisms from both business groups and privacy activists.[3] On October 11, 2019, subsequent California governor Gavin Newsom signed a variety of additional bills aimed at improving the Act. Following a period for public comments on proposed changes to the Act, the California Attorney General submitted a final proposed regulation package to the California Office of Administrative Law for approval on June 1, 2020.[4] The final version of the CCPA largely clarifies certain provisions of the original Act, while also providing exemptions for certain employment and business-to-business related data collection until January 1, 2021.[5] Furthermore, the final Act contains additions meant to harmonize the bill with Civil Code section 1798.99.80, which established a data broker registry created by the California Attorney General.[6]

---

[1] This U.S. Tech Law Update is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This U.S. Tech Law Update may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-474-3258 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: greg@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] The Firm's 2018 U.S. Tech Law Update "California Consumer Privacy Act 2018 – California's GDPR?" can be found here.

[3] CCPA, Cal. Civ. Code §§1798.100 – 1798.199.

[4] CCPA Proposed Regulations, 11 C.C.R. §§999.300 – 999.341.

[5] Assembly Bill No. 25, approved by Governor, October 11, 2019 (2019-2020 Regular Session), clarifies consumer verification procedures for consumer requests and exempts businesses collecting certain employment-related information from the CCPA until 2021; Assembly Bill No. 1355, approved by Governor, October 11, 2019 (2019-2020 Regular Session), clarifies various provisions of the CCPA and exempts business-to-business service-related communications from the CCPA until 2021; Assembly Bill No. 1564, approved by Governor, October 11, 2019 (2019-2020 Regular Session) removes the requirement to have a toll-free number for a business that operates exclusively online and has a direct relationship with the consumers; Assembly Bill No. 874, approved by Governor, October 11, 2019 (2019-2020 Regular Session) clarifies some operative definitions of the CCPA; Assembly Bill No. 1146, approved by Governor, October 11, 2019 (2019-2020 Regular Session), exempts from the CCPA certain scenarios related to vehicle warranty and recall in accordance with federal laws; Assembly Bill No. 1130, approved by Governor October 11, 2019 (2019-2020 Regular Session), revises the definition of personal information to include particular forms of biometric data.

[6] Assembly Bill No. 1202, approved by Governor, October 11, 2019 (2019-2020 Regular Session) requires data brokers to register with the Attorney General.

II. The Final Regulation – More Clarity Than Original Act

The Original CCPA

The CCPA was signed into law by the California governor on June 28, 2018. The Act added sections 1798.100 through 1798.198 to the California Civil Code. Broadly, the CCPA is designed to protect California resident's personal information from use or sale by businesses that fit within particular categories, regardless of whether the business is located in California. The Act also prescribes procedures for business and consumer interaction as they relate to the consumer's rights.

The CCPA explicitly defines the types of businesses required to abide by the Act. In particular, businesses that collect consumers' personal information or determines the purpose and means of processing of consumers' personal information that do business in the state of California must comply with the CCPA if they meet any of the following conditions:

- Has annual gross revenues in excess of US$25,000,000;
- Annually buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
- Derives 50% or more of annual revenues from selling consumers' personal information.[7]

Although the CCPA often references "consumers," most California residents are protected by the CCPA. The Act defines "consumer" as California residents who are in California for other than a temporary or transitory purpose, and individuals domiciled in California who are outside of the state for a temporary or transitory purpose.[8]

Consumer Rights

The CCPA grants consumers certain rights as it relates to their personal information. The "right to know" gives California residents the right to know and access categories and specific pieces of information collected by businesses.[9] The "right to deletion" gives California residents a right to request that a business delete any personal information about the consumer collected by the business.[10] The "right to opt-out/opt-in" relates to the ability of the consumer to opt-in or out of the sale of his or her personal information.[11] Moreover, businesses are prohibited from discriminating against a consumer due to the consumer's exercise of his or her rights under the CCPA.[12]

---

[7] See Cal. Civ. Code § 1798.140(c).
[8] See Cal. Civ. Code §1798.140.
[9] See Cal. Civ. Code § 1798.100; Cal Civ. Code § 1798.110.
[10] See Cal. Civ. Code § 1798.105.
[11] See Cal. Civ. Code § 1798.120.
[12] See Cal. Civ. Code § 1798.125.

Notice Requirements

Furthermore, the final version of the CCPA requires the business to provide a variety of notices to the consumer as it relates to their personal information. In particular, every business that must comply with the CCPA must provide a privacy policy, a "notice at collection," a notice of the right to opt-out, and a notice of financial incentive when businesses offer price or service differences based on a consumer's decision to provide or withhold particular personal information.[13]

The CCPA imposes particular information requirements for privacy policies. Businesses in their privacy policy must, in an easy to read and understandable format, provide consumers with a comprehensive description of the business' online and offline practices regarding the collection, use, disclosure, and sale of personal information and the rights of consumers regarding their personal information.[14]

The "notice at collection" should provide consumers with timely notice about the categories of personal information to be collected and the purposes for which such personal information will be used.[15] A business is required to give this particular notice "at or before the point of collection," and the CCPA clarifies methods in which this is achievable for different types of platforms through which personal information may be collected, such as online, through mobile applications, over telephone, or completely offline.[16] For example, businesses that collect personal information from the consumer online may comply with the notice at collection requirement by providing a conspicuous link to the business' privacy policy on its homepage; conversely, businesses that collect personal information offline may instead provide a paper notice of the notice or post prominent signage directing consumers to an online notice.[17]

Businesses must also provide consumers with a notice of the right to opt-out of sales of their personal information via a "Do Not Sell My Personal Information" link online, or develop another method to achieve the same effect if the business does not have an online presence but collects and sells personal information.[18]

Absent from the original Act but present in the final version is a requirement that businesses give a notice of financial incentive that explains to a consumer the terms of a financial incentive, price or service difference the business offers in relation to the collection, retention or sale of that consumer's personal information.[19]

Consumer Request Procedure

The final version of the CCPA comprehensively lays out procedures for handling consumer requests, partially in response to public comments suggesting considerable confusion

[13] See 11 C.C.R. § 999.304.
[14] See 11 C.C.R. § 999.308.
[15] See 11 C.C.R. § 999.305.
[16] See 11 C.C.R. § 999.305(a)(3).
[17] See 11 C.C.R. § 999.305(a)(2)(e).
[18] See 11 C.C.R. § 999.306.
[19] See 11 C.C.R. § 999.307.

about this issue.[20] The CCPA addresses various different steps in a business' consumer request procedures, including methods of submission by the consumer, methods of response by the business, and methods of verification of the consumer.

Requests to Know and Delete: Businesses must provide two or more designated methods for submitting requests to know and delete, including a toll-free telephone number, unless the business operates exclusively online.[21] When a business receives a request to know or delete, the business must confirm receipt of the request within 10 business days and provide information about how the business will process the request.[22] Beginning on the day that the business receives the request, businesses must respond to the request within 45 calendar days.[23] The CCPA further offers procedures for specific situations, such as when the business cannot verify the identity of the requestor or when a business denies a consumer's request to delete.

Requests to Know and Delete Household Information: Businesses that receive requests to know or delete household information may only do so under certain circumstances. Either the household must have a password-protected account through which the household can submit requests to know and delete, or the household request must meet three conditions. First, all consumers of the household must jointly request access or deletion of household information. Second, the business must *individually* verify all members of the household. Finally, the business must further verify that each member making the request is a current member of the household.[24]

Requests to Opt-Out of Sale of Personal Information: Businesses must provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information."[25] When a business receives a request to opt-out, it must comply with the request as soon as possible but no later than 15 business days after receipt of the request.[26] Additionally, the Act explicitly states that a request to opt-out—unlike other types of requests—does *not* need to be verified; however, the business may deny a request to opt-out if it reasonably suspects the opt-out request is fraudulent.[27]

Requests to Opt-In After Opting Out: Requests to opt-in to the sale of personal information must use a two-step process where consumers can request to opt-in and subsequently confirm their choice.[28] Because the CCPA requires that businesses comply with consumers' opt-out decisions for at least 12 months before requesting the consumer authorize the sale of information, the final Act clarifies that even if the 12 months have yet to pass, a business may inform a consumer who initiates transactions or attempts to use a product or service that requires the sale of personal information that they must opt-in in order to proceed.[29]

---

[20] See California Office of the Attorney General, Final Statement of Reasons, p. 21-45.
[21] See 11 C.C.R. § 999.312.
[22] See 11 C.C.R. § 999.313(a).
[23] See 11 C.C.R. § 999.313(b).
[24] See 11 C.C.R. § 999.318.
[25] See 11 C.C.R. § 999.315(a).
[26] See 11 C.C.R. § 999.315(f).
[27] See 11 C.C.R. § 999.315(h).
[28] See 11 C.C.R. § 999.316.
[29] See 11 C.C.R. § 999.316(b); California Office of the Attorney General, Final Statement of Reasons, p. 40.

Consumer Verification: Generally, all businesses covered by the CCPA must establish, document, and comply with a reasonable method for verifying a requestor is actually the consumer they claim to be. The final CCPA offers several approaches that may be adopted by businesses, and the factors that should be considered when doing so.[30] Businesses are discouraged from requesting additional information from consumers for verification and cannot charge a fee to verify the consumer.[31] Moreover, the CCPA prescribes different verification procedures and examples for password-protected accounts and non-accountholders.[32]

Data Brokers

Following the passage of AB1202, the final CCPA now requires "data brokers," businesses that knowingly collect and sell to third parties the personal information of consumers with whom the business does not have a direct relationship, to register with the California Attorney General on or before January 31 following each year the business fits the definition.[33] Pursuant to the bill, the California Attorney General is tasked with creating a list of data brokers on its website.

In its CCPA Informative Digest, the California Attorney General indicated that the data broker registry is meant to address the problem of consumers not knowing who has and could be selling their information, given that the CCPA does not require businesses to disclose the specific persons or entities with whom they shared the consumer's personal information.[34] The registry publicly identifies specific businesses that may be selling the consumer's personal information so that consumers may exercise their rights over their personal information.

III. "California's GDPR" – Comparisons Between the Act and the EU's GDPR

The CCPA contains significant similarities to the European Union's GDPR, but the core legal framework for each regulation varies. For example, GDPR requires controllers and processors to show a legal basis for processing data—the CCPA does not have similar requirements. Additionally, the CCPA focuses on the sale and transfer of consumer personal data by including explicit procedural requirements, whereas the GDPR's prescribed responsibilities of the data controller and processor apply a broader approach.

Despite some differences, the GDPR and the CCPA largely incorporate the same ideals of personal data protection and individuals' rights over their own data.

	CCPA	GDPR
Protects	**"Consumers"** who are California residents that are either: • In California for other than a temporary or transitory purpose; or	**"Data subjects"** who are in the European Union that can be identified in particular by reference to an identifier such as a name, an identification number, location data, online identifiers, or to open or more

[30] See 11 C.C.R. § 999.323.
[31] See 11 C.C.R. § 999.323 (c) – (d).
[32] See 11 C.C.R. § 999.324; CCR § 999.325.
[33] See Assembly Bill No. 1202.
[34] See California Office of the Attorney General, CCPA Informative Digest.

	• Domiciled in California but currently outside the state for a temporary or transitory purpose. **"Households"** who are people that reside at the same California address, share common devices or services provided by a business, and are identified as sharing the same group account or unique identifier. Cal. Civ. Code § 1798.140(g) 11 C.C.R. § 999.301(h)	factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. GDPR Article 3
Regulates	**"Businesses"** that: • Have annual gross revenues in excess of US$25,000,000; • Annually buy, receive for commercial purposes, sell, or use for commercial purposes the personal information of 50,000 or more consumers; or • Derive 50% or more of annual revenues from selling consumers' personal information. Cal Civ. Code § 1798.140(c)	**"Controllers"** located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which determines the purpose and means of processing of personal data of data subjects. **"Processors"** located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which process personal data of data subjects on behalf of a controller. GDPR Article 24 GDPR Article 28
Types of Data Covered	**"Personal information"** that identifies, relates to, describes, or is capable of being linked to or associated with a particular consumer or household. Non-exhaustive examples include: • Identifiers such as name, postal address, online identifier, IP address, email address, social security number, and other similar identifiers • Characteristics of protected classifications under California or federal law • Commercial information • Biometric information • Internet or electronic network activity information • Geolocation data • Audio, electronic, visual, thermal, olfactory, or similar information	**"Personal data"** that relates to an identified or identifiable data subject. **"Pseudonymized data"** that is processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information when the business also: • Keeps any additional information separately; and • Implements technical and organizational measures to ensure personal data is not attributed to an identified or identifiable data subject.

	• Professional or employment-related information • Education information • Inferences drawn from information Cal. Civ. Code § 1798.140(o)	GDPR Article 3
Types of Data Not Covered	**"Publicly available"** information that is lawfully made available from federal, state, or local government records. **"Deidentified"** information that cannot reasonably identify, relate to, describe, or be linked to or associated with a particular consumer or household when the business also: • Implements technical safeguards that prohibit reidentification; • Implements business process that prohibit and prevent reidentification; and • Makes no attempt to reidentify the information. Cal. Civ. Code § 1798.140(c)(2) – (3) Cal. Civ. Code § 1798.140 (h)	**"Anonymous data"** that cannot be attributed to a specific data subject. GDPR Recital 26
Rights	The right to **"request to know"** what personal information a business has collected about the consumer or household and to whom the personal information has been disclosed. The right to **"request to delete"** personal information about the consumer or household that the business has collected from the consumer. The right to **"request to opt-out"** of the sale of a consumer's personal information by a business to third parties. The right to **"request to opt-in"** of the sale of a consumer's personal information by a business to third parties, with affirmative authorization. The right to non-discrimination for the exercise of a consumer's privacy rights.	**"Right of access"** by the data subject to obtain from controller confirmation as to whether or not personal data concerning the data subject is being processed, and access to the personal data in a readable format. **"Right to rectification"** by the data subject to obtain from the controller the rectification of inaccurate personal data. **"Right of erasure"** by the data subject to obtain from the controller the erasure of personal data concerning him or her without delay, subject to certain conditions. **"Right to restrict processing"** of personal data by the data subject so that the controller can only continue to process the data subject's personal data with the data subject's consent, subject to certain conditions.

	Cal. Civ. Code §§ 1798.100 – 1798.125	**"Right to object"** by the data subject to particular types of processing, including: • Processing necessary for performance of tasks carried out in the public interest; • Processing for direct marketing purposes; and • Processing for scientific or historical research purposes. **"Right to data portability"** by the data subject to transmit personal data provided to a controller to another controller without hindrance. **"Right to lodge a complaint with a supervisory authority"** by the data subject. GDPR Articles 15 – 18 GDPR Articles 20 – 21 GDPR Article 77

Required Notices	**"Privacy policy"** made available to consumers describing the business' practices regarding the collection, use, disclosure, and sale of personal information, and the rights of consumers regarding their own personal information. **"Notice at collection"** given by a business to a consumer at or before the point at which the business collects personal information. **"Notice of right to opt-out"** given by a business informing consumers of their right to opt-out of the sale of their personal information, including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's website or mobile application. **"Notice of financial incentive"** given by a business explaining each financial incentive or price or service difference related to providing personal information. 11 C.C.R. §§ 999.305 – 999.308	Controllers must **provide information** to the data subject, in situations where personal data is collected from the data subject or a third-party. GDPR Articles 13 – 14
Consumer Request Procedures	For **requests to know** and **requests to delete** personal information: • Provide two or more designated methods for submitting requests; • Confirm receipt of consumer requests within 10 business days; and • Respond to requests to know and delete within 45 calendar days, beginning on the day that the business receives the request. For **requests to opt-out**: • Provide "Do Not Sell My Personal Information" link; and • Comply within 15 business days from the date of request receipt. 11 C.C.R. §§ 999.312 – 999.313 11 C.C.R. §§999.317	Controllers must take appropriate measures to communicate with data subjects exercising their rights of access, rectification, erasure, restriction, data portability, and objection in a concise, transparent, intelligible, and easily accessible form. The controller shall facilitate the exercise of data subject rights and allow exercise of data subject rights free of charge. GDPR Article 12

Internal Requirements	All businesses handling personal information must: • Inform individuals responsible for handling consumer inquiries about the requirements in the CCPA and how to direct consumers to exercise their rights; and • Maintain records of consumer requests made pursuant to the CCPA and how the business responded for at least 24 months. Businesses that reasonably should know that it buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year must: • Compile metrics for the previous calendar year as listed in (999.317(g)(1)); • Disclose such metrics by July 1 of every calendar year; and • Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests and compliance with the CCPA. 11 C.C.R. § 999.317	Controllers must maintain records of processing activities under its responsibility. Processors must maintain a record of all categories of processing activities carried out on behalf of a controller (Art. 30). Controllers and processors must conduct a **"data protection impact assessment"** where a type of processing uses new technologies and is likely to result in a high risk to data subjects. (Art. 35). Controllers and processors must appoint a **"data protection officer"** in cases where: • The processing is carried out by a public authority or body; • The core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or • The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses. GDPR Article 30 GDPR Article 35 GDPR Article 37
Security Requirements	No specific security requirements. Businesses must implement and maintain "reasonable" security procedures and practices appropriate to the nature of the information to protect the personal information.	The controller and processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to risk, including as appropriate: • Pseudonymization and encryption of personal data; • The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; • The ability to restore the availability and access to

	Cal. Civ. Code § 1798.150	personal data in a timely manner in the event of a physical or technical accident; and • A process for regularly testing the effectiveness of technical and organizational measures for ensuring processing security. Controllers and processors may demonstrate compliance with security requirements by adhering to an Article 40 **approved code of conduct** or an Article 42 **approved certification mechanism.** GDPR Article 32
Request Verification	Businesses must establish, document, and comply with reasonable method for verifying that the person making a request is the consumer about whom the business has collected information. Generally, businesses should avoid requesting additional information from consumers for verification and cannot charge a fee to verify the consumer. Businesses should also implement reasonable security measures. 11 C.C.R. §999.323	No specific request verification procedures. Controllers should use all reasonable measures to verify the identity of a data subject who requests access. GDPR Recital 64
Minors	Businesses with personal information of **minors under 13 years of age** must establish, document, and comply with a reasonable method for determining and receiving affirmative authorization from the minor's parent or guardian to opt-in to the sale of their personal information. Businesses with personal information of **minors at least 13 and less than 16 years of age** shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information. 11 C.C.R. §§ 999.330 – 999.332	Processing of personal data of **minors below 16 years of age** must be consented to by the minor's parent or guardian. GDPR Article 8
Valuing Data	Businesses offering financial incentive or price or service difference must use and document a reasonable and good faith	The GDPR does not require controllers or processors to calculate the value of personal data.

	method for calculating the value of the consumer's data. 11 C.C.R. § 999.337	
Data Breaches	No explicit procedural requirements.	Controllers and processors must notify the supervisory authority. When the data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller must communicate information about the breach to the data subjects. GDPR Articles 33 – 34
Penalties	The California Attorney General may **implement fines** ranging between US$2,500 for non-intentional violations and US$7,500 for intentional violations (1798.155). Consumers may initiate **civil actions** for: • Recovery of damages in an amount not less than US$100 and not greater than US$750 per consumer per incident or actual damages, whichever is greater. • Injunctive or declaratory relief, or any other relief the court deems proper. Cal. Civ. Code § 1798.150 Cal. Civ. Code § 1798.155	The supervisory authority may **implement fines** of up to EUR€10,000,000 or 2% of total worldwide annual turnover for the preceding financial year for smaller infractions, and up to EUR€20,000,000 or 4% of total worldwide annual turnover for the preceding financial year for larger infractions (Art. 83). Data subjects may initiate **civil actions** for an effective judicial remedy (Art. 79). GDPR Article 79 GDPR Article 83