The California Consumer Privacy Act: The ethos, similarities and differences vis-a-vis the General Data Protection Regulation and the road ahead in light of California Privacy Rights Act

Received: 24th February, 2021

Tripti Dhar
Partner, Reina Legal LLP, India

Tripti is a partner at Reina Legal LLP and heads the Data Protection and Privacy practice for India, EMEA and USA. She is an alumnus of NALSAR University of Law, Hyderabad, India and has a work experience of more than nine years in Information Technology (IT) and TMT. She is a Fellow of Information Privacy (FIP) as designated by the International Association of Privacy Professionals (IAPP) and holds the CIPP/E and CIPM certifications. She is also a certified ISO 27001 Lead Auditor as issued by the British Standards Institute (BSI). She is admitted to practice in the courts of India and has previously advised clients across the sectors of, inter-alia, IT, TMT, healthcare, hospitality, fintech, media and entertainment. She has undertaken many speaking engagements in and conducted trainings and workshops across various sectors. Tripti's core focus area is evolving data protection law and jurisprudence across the globe.

20th Floor, WeWork, Oberoi Commerz II, International Business Park, Oberoi Garden City, Off WEH, Goregaon East, Mumbai–400063, Maharashtra, India
Tel: +91 9871 268235; E-mail: Tripti.Dhar@outlook.com

Abstract Amidst the ongoing privacy concerns, legislations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have given individuals the insight into their personal data and a control thereof. These legislations, however, must not be viewed as impediment to business but as business enablers that ensure successful conduct of business while balancing the rights of the individuals vis-à-vis that of the businesses. This paper seeks to delve into the spirit and the most striking features of CCPA. The paper also aims to compare the GDPR and CCPA so as to ascertain the key similarities and key differences between the two. The paper finally attempts to trace the journey of global companies in the quest to achieve compliance before 1st January, 2020. As of today, businesses are faced with a peculiar circumstance. They have aligned their businesses in line with the GDPR and are now also required to align with the obligations under CCPA. The procedural aspect has the business taken by storm. To make matters complicated, businesses are now faced by the California Privacy Rights Act (CPRA) and the relevant compliances expected of them. The paper seeks to conclude with a roadmap for global businesses in such a factual matrix.

KEYWORDS: CCPA, GDPR, CPRA, data protection, data privacy

INTRODUCTION

The ever-increasing reliance of global businesses on personal information or personal data of consumers has also resulted in frequent occurrence of data breaches due to the sheer magnitude of the data collected and perhaps due to the efforts in protecting the same not matching up. The constant reporting of such data breaches has left with the consumers an increased sense of vulnerability in the face of businesses. The idea of having a legislation in place is twofold: first, to empower the consumers and assuage their concerns as to their personal data and secondly, to enable and empower businesses by giving them a framework to operate within. Let us take a step back and assess the need for a legislation altogether. The need arises when the society or a section thereof is faced with a peculiar set of circumstances in which a legal relationship is to be casted, rights need to be determined and obligations need to be set upon. A legislation seeks to organise a society and protect its citizens. Amid the ongoing privacy concerns, legislations like General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have given the individuals and consumers, respectively, the insight into their personal data/ information and control thereof. The data protection and privacy legislations must not be viewed as impediment to business but as business enablers that ensure successful conduct of business while balancing the rights of the individuals vis-à-vis that of the businesses.

The state of California in the United States has introduced a legislation that seeks to enable businesses that use personal data of consumers for various legitimate purposes, while balancing the rights of such consumers. California is the fifth largest economy in the world[1] with its gross domestic product at US$2,968bn. The residents of California are a massive market in themselves, and realising the same, the CCPA is set to protect California consumers by empowering them with a host of new data privacy rights. The manner in which these rights are drawn, the CCPA is anticipated to be nothing short of a game changer for businesses which will have to brace themselves up.

In this background, this paper seeks to empower the readers with:

a. a synopsis of the ethos of the CCPA;
b. key similarities between the GDPR and the CCPA;
c. key points of divergence between the GDPR and the CCPA; and
d. road ahead for the global businesses

Note: It is pertinent to mention here that due efforts have been made to incorporate latest developments around CCPA and GDPR. As the legislations of CCPA and GDPR are vast, best efforts have been made to touch on briefly the key topics of relevance to the readers.

CCPA — core elements

The ethos of CCPA is to protect California residents by granting them new rights with respect to their personal information. The law acknowledges that businesses collect personal information of consumers and use them for profit. This collection and processing for profit should be undertaken only on express consent of the consumer. Hence, the opt out of sale or Do Not Sell My Personal Information' link is mandated to be displayed on the website of all the businesses seeking to do business in California. The personal information in this realm is characterised by some specific inclusions, such as information linked with household or a device, and specific exclusions, like personal information such as medical information and information collected as a part of clinical trials that fall within the ambit of other sectoral legislations.

Consumer	Business	Selling of personal information	New privacy rights	New penalties and damages	Right against discrimination
1. You need to be a California resident (residency as defined in the taxation statute). 2. An individual/household/device.	1. A 'for-profit' business across the globe. 2. Doing business in California. 3. Exceeding the prescribed threshold.	1. Certain new disclosure requirements regarding selling of personal information. 2. Mandating of a specific 'opt out'.	1. New privacy rights conferred on consumers—right to access, deletion and portability of personal information.	1. Introduction of new penalties and statutory damages in case of data security breaches.	1. A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights.

It also carves out an exclusion of transfer of data to a third party in the context of a merger from the definition of selling personal information, sale of information to or from consumer reporting agencies, personal information under the Graham–Leach–Billey Act, personal information under the Driver's Privacy Protection Act and personal information in the public domain lawfully made available from federal, state or local. The CCPA grants to the consumers the right to access their personal information, to have it deleted and to opt out of the sale of their personal information. As a result, the businesses are required to have systemic and technical capabilities to accommodate the solutions tied to these rights, and hence, CCPA is viewed to have considerable impact on all commercial enterprises that have been conducting business in California up until now. A very strong right that has been granted to consumers under the CCPA in no ambiguous terms is that of protection against discrimination. The CCPA states that by the virtue of the fact that consumers have exercised their rights under the CCPA, they must not be subjected to any kind of discrimination.[2] An illustrative list of behaviour by the businesses that can be viewed as discriminatory are (a) denying goods or services to the consumer, (b) differential pricing of goods or services either through discounts or other benefits or through imposing penalties, (c) provision of differential level or quality of goods or services to the consumer and (d) suggesting differential pricing or level or quality of goods or services. This, to me, is the most telling feature of the CCPA. This is the spirit of the consumer protection that CCPA seeks to percolate into the businesses. It involves not only giving the consumer potent tools to protect and control their personal information and use thereof but also ensuring that the consumers do not suffer as a result of exercising these rights. This in-built mechanism is akin to the green light theory, if it may be said so, wherein the focus is on encouraging efficiency within existing systems rather than post facto enforcement.

A snapshot of the core elements of CCPA are presented as the above.

ATTORNEY GENERAL'S PROPOSED REGULATIONS: A STEP TOWARDS GREATER CLARITY?

The Attorney General of California (AG), Xavier Becerra, on 10th October, 2019, issued proposed regulations under the California Consumer Privacy Act of 2018[3] for public consultation ('Proposed Regulations'). Under the Proposed Regulations, guidance with respect to the practical implementation of the CCPA and the approach that the AG's office would take towards compliance requirements under the CCPA have been elaborated upon. The key issues addressed are (a) clarificatory

definitions; (b) notices required to be provided by businesses to consumers; (c) the consumer requests made to the businesses and verification thereof; (d) business practices regarding the personal information of minors and (e) nondiscrimination.

A. Definitions

Certain clarificatory definitions have been introduced by way of the Proposed Regulations, which enable a better understanding of the terms used in the CCPA. The key definitions that aid in a better understanding of the intent of the legislators are (a) household; (b) categories of third parties; (c) privacy policy; (d) financial incentive and (e) third-party identity verification service.

B. Notice to consumers

The Proposed Regulations explain in detail the procedures that must be followed when businesses provide specific notices[4] to consumers. The specified notices are as follows:

a. Section 999.305 — Notice at Collection of Personal Information[5]
b. Section 999.306 — Notice of Right to Opt-Out of Sale of Personal Information[6]
c. Section 999.307 — Notice of Financial Incentive[7]
d. Section 999.308 — Privacy Policy[8]

The common thread running through all the aforementioned notices is that they must be designed and presented to the consumer in such a way that is easy to read and understandable to an average reader. Businesses are required to use plain, straightforward language and avoid any technical or legal jargon, and it is also required that the notices 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 emphasise that businesses must follow the core principles of transparency and purpose limitation and should not collect categories of personal information other than those disclosed in the notice at collection.

Businesses that do not collect information directly from consumers are not obliged to provide notices at collection to the consumer; before the sale of such personal information, however, they must either (a) contact the consumer directly with regard to the sale of information and provide the right to opt out or (b) 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.

Exemption from Providing Notice of Right to Opt Out

The key clarifications sought to be brought in by the Propose Regulations are the conditions under which a business is exempt from providing a notice of right to opt out. There are two conditions[9]:

a. It does not, and will not, sell personal information collected during the time period during which the notice of right to opt out is not posted; and
b. It states in its privacy policy that it does not and will not sell personal information.

It must be noted that a consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt out.

C. Business practices for handling consumer requests — verification and response

Vide the Proposed Regulations,[10] detailed business practices to be employed while handling consumer requests, and their

verification have been elaborated and clarified. A snapshot of these detailed practices is as follows:

a. Section 999.312 — Methods for Submitting Requests to Know and Requests to Delete
b. Section 999.313 — Responding to Requests to Know and Requests to Delete
c. Section 999.314 — Service Providers
d. Section 999.315 — Requests to Opt-Out
e. Section. 999.316 — Requests to Opt-In After Opting Out of the Sale of Personal Information
f. Section 999.317 — Training; Record-Keeping
g. Section 999.318 — Requests to Access or Delete Household Information

Verification of Requests[11]

a. Section. 999.323 — General Rules Regarding Verification
b. Section. 999.324 — Verification for Password-Protected Accounts
c. Section. 999.325 — Verification for Non-Accountholders
d. Section. 999.326 — Authorized Agent

Vide the Proposed Regulations, the abovementioned practices have brought clarity 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. Readers are encouraged to refer to the Articles 3 and 4 of the Proposed Regulations to maintain brevity in this paper.

D. Business practices regarding the personal information of minors

Vide the Proposed Regulations, some special rules have been provided for business practices regarding Personal Information of Minors[12]

a. Section 999.330 — Minors Under 13 Years of Age
b. Section 999.331 — Minors 13 to 16 Years of Age
c. Section 999.332 — Notices to Minors Under 16 Years of Age

Minors under 13 years of Age

In the event that 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 authorising 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 which 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.

Minors 13–16 years of Age

For minors 13–16 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.

Notice to Minors under 16 years of Age

Businesses that exclusively target offers of goods or services directly to consumers

under 16 years of age and do not sell the personal information of such minors without their affirmative authorisation, or the affirmative authorisation of their parent or guardian for minors under 13 years of age, are not required to provide the notice of right to opt out.

E. Nondiscrimination[13]

This paper proposes to further clarify Section 1798.125 of the CCPA. Vide the Proposed Regulations, the following detailed guidance and clarifications have been provided:

a. Section 999.336 — Discriminatory Practice
b. Section 999.337— Calculating the Value of Consumer Data

A financial incentive or a price or service difference is considered discriminatory and, therefore, prohibited when a business treats a consumer differently by virtue of the consumer having exercised a right conferred by the CCPA or the Proposed Regulations. A business, however, may offer a price or service difference in the event and only if it is reasonably related to the value of the consumer's data.

Such value may be calculated by using certain prescribed factors like 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.

SIMILAR ASPECTS

A. Individuals as the pivot — the law transcends boundaries

GDPR — Article 4(1) | CCPA— Section 1798.140(g)

The CCPA and the GDPR both seek to protect the personal data of individuals within their respective jurisdictions. Both laws transcend the conventional jurisdictional boundaries of law in as much as that they have made the individuals as the pivot of a commercial transaction arising out of such individual's personal data/ information. The very fulcrum of both the legislations is protection of personal data and to place the control of the personal data in the hands of the respective individuals regardless of where the businesses dealing with the individuals are located. The impact of both CCPA and the GDPR is global.

B. Crucial terminologies and definitions

Personal Data/Personal Information

GDPR — Articles 4(1), 9(1) Recitals 26–30 | CCPA — Section 1798.140(o), Sections 1798.145 (c)–(f)

The GDPR defines personal data to be any information relating to an identified or an identifiable data subject. The manner in which CCPA defines personal information is that it identifies, relates to, describes, is capable of being associated with or could reasonably be linked with, directly or indirectly, a particular consumer or household. This definition is followed by a detailed list of specific categories of personal information. While the definition of personal data under the GDPR is substantially similar to the definition of personal information under the CCPA, the latter seeks to include under its purview, information linked with a household and a device.

Actors at Play — Controllers/Businesses and Processors/ Service Providers

GDPR — Articles 3, 4(1) Recitals 90, 93 | CCPA — 1798.105, 1798.140, 1798.145, 1798.155

Controllers or businesses are the organisations that determine the purpose and means of the processing of data. Processors

or service providers are organisations processing personal data on behalf of the controllers.

It is important to note that both the GDPR and the CCPA are legislations aimed at containing the 'malaise' of surveillance capitalism. In today's time, the commodity for sale is an individual's personal data, and the analytics of the data so obtained relies on the mass surveillance of individuals on the internet. In the light of a series of breaches, where big corporations across sectors have been caught in the fray, it may be said that the GDPR and the CCPA are social-welfare legislations not in its conventional sense but in a more context-appropriate sense. These big corporations may at times be a controller or simply be a processor or both; the respective legislature, however, has taken due notice of this fact and accordingly incorporated provisions to prevent unnecessary and unlawful monitoring of behaviour of individuals for pure capitalist ends.

Accordingly, the actors at play under the GDPR are regulated regardless of their establishment in the European Union (EU). In the event, the actors have an establishment in EU and process the data of EU irrespective of the fact whether such processing takes place in the EU. The actors are not established in the EU but process personal data of data subjects who are in the union where the processing activities are related to (a) offering of goods or services to such data subjects, irrespective of whether a payment from such data subject is required, or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.

Under both the GDPR and the CCPA, in order for personal data/personal information change hands from the controller to the processor, a definitive and written contract is required to be in place detailing the relationship between scope, roles, tasks and obligations of the controllers and the processors.

The data controllers in the scheme of the GDPR are similar to businesses in the scheme of CCPA. While the role of both is largely the same, CCPA seeks to identify with certainty the controllers and processors it seeks to regulate, and hence, certain detailed criteria like the entity being 'for-profit', prescribing of threshold, etc., are built in the legislation.

The GDPR prescribes in great details activities that are required to be undertaken by the actors, such as record-keeping, conducting data protection impact assessments, appointing a data protection officer (DPO), notification obligations on breach. The CCPA on the other hand has at its core the obligation to prevent unlawful selling of the personal information of its consumers, and hence this very aspect has been detailed in the CCPA (again, to contain the malaise of surveillance capitalism).

Under the GDPR, the obligations of processors are defined and detailed. They are recognised as crucial actors having their own set of activities during processing, and hence, obligations for those set of activities are imposed on the processors directly. The CCPA does not impose any direct obligations of the service providers.

Pseudonymisation and Anonymisation

GDPR — Article 4(5), 11 Recitals 26, 28 | CCPA — Sections 1798.100(e), 1798.140(r), 1798.145(i)

Under both the legislations, it is mandated that appropriate technical and organisational controls are put in place to prevent reidentification of personal data that has been removed of its identification.

Under the GDPR, it is crystal clear that personal data which has undergone pseudonymisation and which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person. Similarly, GDPR is also clear that

anonymised data is not considered personal data and is outside of its purview.

Under the CCPA, three specific terms have been used. They are aggregate consumer information [Section 1798.140(a)], deidentified [Section 1798.140(h)] and pseudonymize or pseudonymization [Section 1798.140(r)]. While the intent behind the legislature is expected to perhaps relax the obligations of businesses and service providers, it cannot be said so with certainty. The thread holding these three concepts together in the CCPA is the prevention from reidentification of personal data. So, while CCPA does not place any restriction on a business to collect, use, retain, sell or disclose a personal information that is aggregated or deidentified, to call a particular data as aggregated or deidentified requires a high level of treatment of data if it may be so called. In so far as pseudonymised data is concerned, because of its very nature of being identified with provision of additional information, we can expect clarity from subsequent interpretations that pseudonymised data folds within personal data.

While under both the GDPR and the CCPA the data controller is not expected to reidentify data and maintain additional data with itself to reidentify this pseudonymised data, GDPR provides an exception to the effect that in case a data subject requests for its rights and also provides additional information to the controller, the controller in order to comply with the data subject request has to reidentify the data. The CCPA does not require businesses to honour such a consumer request with reidentifying or otherwise linking information that is not maintained in a manner to call it personal information.

This study compels a conclusion that as interpretations under the CCPA will be made, the intent of both the legislations on this front shall be more similar than different.

Research — Scientific, Historic, Statistical Purposes

GDPR — Article 5(1)(b), 9(2)(j), 14(5), 17(3)(d), 89 Recitals 33, 159,160,161 | CCPA — 1798.105(d)(6), 1798.140(d)(6)

Under both the legislations, personal data that is collected for specified, explicit and legitimate purpose when processed further for scientific or historical research purpose shall not be considered as incompatible with the original purpose (CCPA excludes clinical trials from the scope). Appropriate safeguards to ensure the rights of the data subjects are expected to be maintained and employed by the data controllers. While GDPR recommends pseudonymisation in this regard, CCPA has imposed a specific set of safeguards like pseudonymisation, deidentification, having technical safeguards and additional security controls in place, noncommercial use, etc. The legislations also provide the right of erasure/deletion not to apply to processing for the purposes of research if the erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing.

Third Parties

GDPR — Article 4(10) | CCPA — Section 1798.140 (w)

Under the GDPR, a third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Quite converse to it, under the CCPA, a third party is defined in a negative way, ie the CCPA defines what a third party is not. Thus, 'third party' is a person who is not any of the following:

1. The business that collects personal information from consumers under the CCPA; or

2. A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, where the contract provides that the party's use of personal information should prohibit that person from:
   a. Selling the personal information;
   b. Retaining, using or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract; and
   c. Retaining, using or disclosing the information outside of the direct business relationship between the person and the business.

Any such third party receiving the personal information must certify that they understand the abovementioned limitations and will comply with them.

Interestingly, the Proposed Regulations define 'Categories of third parties'[14] means 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.

A business shall 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. The business shall notify the consumer when this has been completed[15]

The third-party compliances or obligations of data controllers/businesses vis-à-vis data subjects/consumers where third parties are employed are treated under GDPR, and CCPA has been mentioned in this paper in various paragraphs.

Let us consider the current position of the third parties and challenge posed to the data controllers/businesses. It is accepted that oftentimes there are challenges in identifying third parties from processors. The thin line between a processor/service provider and a third party has been a subject of debate. The way a third-party vendor is defined becomes important as a business is required to make the relevant disclosures with regard to third parties, but the same requirement does not apply to service providers. Opposite to it, businesses are obligated to require service providers to delete personal information when a consumer requests the business to do so; they do not, however, have the same requirement regarding third parties.

In order for businesses to be able to effectively comply, it is required to be determined as to which vendors qualify to be third parties and the compliances accordingly be then set in process. Hence, it is recommended that when drafting vendor agreements and formulating the privacy notice, the distinction between the third parties and service/provider processor should be made out clearly, and their role and their relationship with the data controller must be spelt out clearly. The privacy notice should contain in clear terms all the disclosure requirements and how the relevant processing is linked with the purpose for which the personal information is sought to be collected.

C. The bouquet of rights available to the individuals

The right to access personal information has been granted under both the legislations. Within the right to access is a bouquet of rights. These are right to access, correct, to be informed and delete personal data.

Under both the legislations, the right of access is not an absolute right but is qualified and may not be granted in certain circumstances. For instance, the individuals have a right of access to correction or deletion of their personal information but not if that access or correction or deletion adversely affects the rights and freedoms of others or is prohibited under other specialised

legislations in the realm of national security or banking and securities law.

Right of Access

GDPR — Articles 12, 15, 20 Recitals 59, 63, 64 | CCPA — Sections 1798.100, 1798.105, 1798.110, 1798.130

The right of access to one's own personal data is granted by both the GDPR and the CCPA. This right enables an individual to know of the data that a controller or a processor may hold about them. Emphasis on existing capabilities and mechanisms to ascertain that the access request is genuine and of the same data subject is maintained in both the legislations. While the spirit of this right is same in both the legislations, the procedures of providing access may vary, which have been delineated in the table below:

Right to Be Informed

GDPR — Articles 5, 12, 13, 14 Recitals 58–63 | CCPA — Sections 1798.100 (b), 1798.130(a), 1798.135

Both the legislations mandate that the individuals be informed as to when their personal data is being collected along with the prescribed details of such collection and/or processing. While both the legislations have similar requirements of disclosure to individuals, the GDPR requires detailed information about the activity of personal data collection and processing, the emphasis being more on the actors involved in the activities and whether the data is collected from the individual directly or through a third party. CCPA, on the other hand, requires disclosure of specific information to the individuals that pertains to the categories of personal data collected and the intended use thereof. Hence, it can be concluded that overarchingly both CCPA and GDPR have emphasised on appropriate disclosures to the individuals. A privacy notice that is the mode of informing the individuals will have certain similarities and certain differences as well. While the similarities under the respective legislations have been discussed here, the point of departure of the two legislations within the 'right to be informed' is discussed in greater details in the section of the differences ensuing between the CCPA and the GDPR.

S.No.	GDPR	CCPA
1.	Upon a data subject making a request to access its data, the data controller is required to communicate the following: a. Purposes of the processing b. Categories of the processing c. The recipients or the categories of recipients to whom disclosures have been made d. Sources from which the data has been collected (if not collected on own) e. The retention period f. Right to complaint before the supervisory authority g. Possibility of data transfers	Upon a consumer making a request to access its data, the business must communicate the following: a. Categories of personal information collected or sold b. Categories of sources from where personal information was collected c. The business or commercial purpose for collecting or selling personal information d. The categories of third parties with whom business shares personal information e. The specific pieces of personal information that the business has collected about the consumer
2.	The form in which a data subject can request access is manifold, and when the request is made through electronic means, the data controller is mandated to respond through the same.	Consumers are required to give at least two methods to make their request. These methods may be through a toll-free phone or a webpage. The business can send its response through electronic means.
3.	This right can be exercised free of any charge unless the requests are unfounded, excessive or repetitive in nature.	This right can be exercised free of any charge unless the requests are unfounded, excessive or repetitive in nature.

Right of Deletion

GDPR — Articles 12, 17 Recitals 59, 65 and 66 | CCPA — 1798.105, 1798.130(a) and 1798.145(g)(3)

The right to deletion of personal data is also similar under both the legislations to the effect that it is a requisite under both the laws that the individuals be made aware of their right to ask for deletion/erasure of their personal date. What is strikingly similar is also the scope of this right which travels not only to the data controllers but also to the third parties like data processors, recipients, subprocessors, parties to whom data has been sold, etc. Moreover, individuals can exercise this right free of any fee, unless it is found that the requests of the individual are excessive or repetitive in nature. It is also mandated by both the legislations that the data controllers have such in-built mechanisms in place which ensure that the deletion requests are genuine and from the concerned individual. The exceptions that are carved out of the right of deletion are (a) freedom of expression; (b) research purposes; (c) compliance with legal obligation and (d) necessary in exercise of a legal claim or against an illegal activity.

Data Security

GDPR — Article 24(1) | CCPA — 1798.150 (a)(1)

While both the legislations do not legislate specifically on the aspect of data security, GDPR expects that the controllers and processors will employ appropriate technical and organisational measures [Article 24(1) of the GDPR]. The CCPA does not specifically impose any data security requirements on the businesses or service providers; as there exists a remedy under the CCPA with respect to certain data breaches like unauthorised access and exfiltration, theft or disclosure resulting from the violations of a business's duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information, however, a consumer may institute a civil suit, and it is evident that to implement the CCPA in its true spirit would require the businesses to have appropriate data security measures in place.

KEY DIFFERENTIATING ASPECTS

A. Personal data/personal information

GDPR — Articles 4(1), 9(1) Recitals 26–30 | CCPA — Section 1798.140(o), Sections 1798.145 (c)–(f)

The point of departure of GDPR and CCPA in so far as personal data is concerned is that the GDPR seeks to apply all the requirements of compliance prescribed under it to publicly available information. CCPA, on the other hand, seeks to keep out of its purview such publicly available information which is lawfully made available from the federal, state or local government records. An exception to this is the biometric data collected by businesses without taking the necessary permission of the consumers.

While GDPR carves out a special standard for and prohibits processing of special categories of personal data like health-related personal data, CCPA excludes medical information and personal information collected during clinical trials from its ambit as these are already covered by either special or sectoral legislations.

Under the GDPR, as discussed earlier, processing of special categories of personal data is prohibited. The special category includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and mandates that processing of the aforementioned personal data is prohibited. The CCPA does not carve out or categorise a special category

in a manner similar to GDPR or does not provide specific rules for collecting or processing or sharing of biometric data. As mentioned in foregoing paragraphs, 'publicly available information' does not include biometric data collected by businesses without taking the due permission from consumers.

B. Legal basis of processing personal data

GDPR — Articles 5–10 Recitals 39–48 | CCPA — Section 1798.120

Under the GDPR, any processing of personal data is permitted and is lawful only on fulfilment of either of the six grounds laid down under Article 6. These are (a) consent; (b) performance of contract; (c) compliance with a legal obligation; (d) to protect the vital interests of the data subject or any other natural person; (e) public interest or in exercise of official authority vested in the controller and (f) processing for legitimate interest pursued by the controller or a third party.

In what can be termed a stark contrast, CCPA only provides for post facto safeguards for processing personal data at the time of (a) sale of their personal information; or (b) disclosure of their personal information or (c) making requests for erasure of their personal information.

Again, as the overall ethos of the CCPA is to regulate the sale of personal information of consumers, a focused approach has been employed throughout the legislation.

C. Right of access

GDPR — Articles 12, 15, 20 Recitals 59, 63, 64 | CCPA — Sections 1798.100, 1798.105, 1798.110, 1798.130

Certain points of departure in right to access have been found. CCPA mandates that a consumer can access its personal information collected in the 12 months prior to the request made, where under GDPR, the right to access is extended to all personal data of a data subject collected and processed. This necessarily means that under the CCPA, a business can refuse to respond to the request of a consumer which pertains to its data collected before a period of 12 months from the date of request. The data controllers have no such right under the GDPR; they can, however, refuse to honour the data subject access requests only in the event if they are manifestly unfounded, excessive or repetitive in character.

The timelines to respond under both the legislations vary. While GDPR mandates that data subject requests must be complied without any 'undue delay', an outer limit of one month from the date of receipt of request is prescribed. In the event of complex requests, an extension of two months can be provided, provided the data subject is informed of such an extension within the initial deadline of one month. The timeline under the CCPA is that of 45 days from the date of receipt of a consumer's request. An extension of another 45[16] days is permitted under the CCPA provided that the notice of such extension is given to the consumer within the 45-day period.

D. Right to data portability

Articles 20 Recital 68 | CCPA — Sections 1798.100, 1798.130

While CCPA has beautifully woven the right of data portability into right of access and mandates that, wherever technically feasible, the provision of personal data by the businesses to the consumers in a portable and readily usable format, the GDPR has a separate provision for data portability which sets in under specific circumstances. This separate right under the GDPR mandates that a data subject has the right to receive its data in a structured, commonly used and machine-readable format so as to enable smooth transmission of the personal data to third parties.

GDPR, however, has very meticulously carved out that the right to portability is

S.No.	GDPR	CCPA
1.	All lawful grounds (and not only consent) are applicable for processing of personal data of a child.	Only consent is the lawful basis of selling personal information of a child.
2.	Processing of personal data of a child shall be lawful where the child is at least 16 years of age.	A business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age without its consent.
3.	Right to opt in is the general norm a. A child below the age of 16 years, processing shall be lawful only if and to the extent that consent is given or authorised by its parents or guardian. b. Member states have been given the leave to provide by law for a lower age provided that such lower age is not below 13 years.	Right to opt in only in case of children a. The children in the age group of 13–16 years are required to affirmatively authorise such sale of personal information. b. For the children less than 13 years of age, their parent or guardian is required to affirmatively authorise the sale of personal information.
4.	No exception is provided for a data controller that is not in know of the fact that it is providing services to a child. Provision of appropriate information to the child, an appropriate privacy notice in plain and clear language to be in place and specific attention be given to public awareness and understanding of risks, rules, safeguards and rights in relation to processing.	A business that wilfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

applicable only (a) to the extent of the personal data that has been shared by the data subject itself; (b) such personal data is processed on the premise of consent or contract and (c) the processing is carried out by automated means.

Another departure is that GDPR has permitted within data portability request, the flow of personal data in a portable form, upon data subject's request, from one controller to another. CCPA, however, has limited data portability to only provision of the consumer data to the consumer itself.

E. Child

GDPR — Articles 8, 40, 57 recitals 38, 58, 75 | CCPA — Sections 1798.120(c) and (d)

There is a marked difference in the manner the personal data of children is treated under the GDPR and the CCPA. While the GDPR captures the law on all processing of personal data of children, CCPA seeks to address only the selling of personal information of children. It is pertinent to note that obligations towards a child under CCPA are in addition to and not in derogation of the obligations under the Children's Online Privacy Protection Act ('COPPA'). A tabular representation attempts to capture key differences.

F. Right to be informed/privacy notice

GDPR — Articles 5,12, 13, 14 Recitals 58–63| CCPA — Sections 1798.100(b), 1798.130(a), 1798.135

A very important right for data controllers and consumers is the right to be informed. This is a very important right as this is the first contact that the data controller has with its data subject, and hence, for a business to be compliant with these two legislations, this will be one of the most crucial aspects to get right, the delivery of information to the data subject. A privacy notice is the mode of informing the consumers. The

S.No.	GDPR	CCPA
1.	At the time when personal data is collected, the data controller is required to provide the data subject with details with respect to the data collection and data processing activity. Subsequent notice to be provided by the controller to a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/obtained.	Consumers to be informed about a. The personal information categories collected b. The purposes for each category that the personal information collected for is used Subsequent notice to be provided in order to a. Collect any additional personal information categories b. Use any information collected for purposes other than specified for before
2	Privacy notice to contain • Identity of the controller • Contact details of the data protection officer (DPO) • Purpose of processing for which the personal data is intended as well as the legal basis for processing • Legitimate interest of the data controller or the third party • The recipient or the categories of data • Transfer of data to third parties • Data retention period • Right to access to and rectification or erasure of personal data or restriction of processing or object to processing as well as data portability • Right of withdrawal of consent • Right of complaint before the supervisory authority • Consequence of nonperformance of contract where it is the lawful ground of processing • Automated decision making, if any.	• Categories of personal information either collected or sold or disclosed to third parties for the purposes of business in the past 12 months. • Privacy notice online or otherwise is required to be updated every 12 months. • If no personal information is/was sold, then it should be written in the privacy policy.
3.	• Specific information must be given to the data subject at the time of collection of data by a third party.	• An explicit notice to be given to the consumers at the time a third party intends to sell personal information about that consumer that has been sold to the third party by a business.

crucial differences between the delivery of information mandated under the GDPR and the CCPA, respectively, translate into different requirements of a privacy notice. These differences have been listed.

G. Right to object to and restriction of processing opt out of selling of their personal data

GDPR — Articles 18 and 21 |CCPA — Section 1798.120

The general scheme of the GDPR is that of an 'opt-in' consent; on the converse, CCPA has laid down the scheme of 'opt-out' consent, with the exception of personal information of children. It is to be borne in mind that under the GDPR, the 'opt-out' is only from the selling of their personal information and not other activities like collection, processing, etc., against which data subjects of GDPR can object. So, the right to object under the GDPR is broader than that under the CCPA.

The right of objection that is granted under the legislations is that a data subject can object to his data being processed, while under the CCPA, the consumer can object to his personal information being sold, and hence, the actor has to immediately stop his activity of processing or selling. In order to further this objective, CCPA has mandated that a notice saying 'Do Not Sell My Personal Information' be given to the consumers. This is seen as the right of the

consumers to direct a business, at any time, to not sell the personal information of a consumer to a third party. A lot of debate is going around as to how to make companies compliant with this requirement under the CCPA as this compliance is the most visible one as it is always supposed to be displayed to the customers (on the homepage of their website) and will be in public domain.

H. Right of rectification

GDPR — Article 16 | CCPA — None

An explicit right has been granted to the individuals under the GDPR where the individuals can (a) correct any inaccuracies in their personal data and (b) remedy any incompleteness in their personal data. In so far as the CCPA is concerned, there is no particular provision in the law that mandates the businesses to rectify the personal information of the consumers collected.

I. Right not to be subject to discrimination by virtue of exercise of rights

GDPR — Articles 5, 13 and 22 Recitals 39, 71, 72 | CCPA — Section 1798.125

As mentioned previously, the right not to be subject to discrimination is a hallmark right under the CCPA. The CCPA mandates that a business should not discriminate against a consumer due to the fact that he or she exercised its rights under the legislation. A host of possible ways in which discrimination can be affected has been laid out in the legislation.[17] CCPA, however, also posits that a business may charge a consumer differently or provide a different level or quality of goods or services if the difference is reasonably related to the value provided by the consumer's personal data. Conversely, if a consumer were to give the business prior opt-in consent, a business may offer financial incentives to such consumers.

While the GDPR may not provide this right in so many words, the spirit of anti-discriminatory behaviour towards data subjects is implicit in the legislation, eg GDPR maintains that lawfulness and fairness are the touchstones of processing of personal data. The GDPR also protects its data subjects against any such decision that is based solely on an automated processing,[18] including profiling, so as to produce legal effects concerning the data subjects.

J. Independent supervisory authorities

GDPR — Articles 51–84 Recitals 117–140 | CCPA — Sections 1798.155, 1798.185

Under the GDPR, the data protection authorities are the supervisory authorities. They are bodies that guide the various stakeholders regarding their roles, responsibilities and obligations under the GDPR. These are specialist bodies created under the mandate of the GDPR. The supervisory authority under the CCPA is the AG, and it is he/she who is mandated to create regulations on, but not limited to, the specific areas of the CCPA. The authorities under the GDPR have wide, detailed and express powers to conduct audits, access all the data necessary for performance of tasks, obtain access to the premises of the controller or the processor, issue warnings, order compliance, direct communication of a data breach to the data subject, put a ban on processing of data, order rectification of erasure of data, impose fine, etc. These are wide, investigative and remedial powers. On the other hand, the AG has the blanket power to assess a violation, impose monetary penalties and injunctions under the CCPA. While this is not a very detailed power, it can encompass most of the activities that should be provided to a supervisory authority.

K. Remedies and penalties

Civil remedies

GDPR — Article 82 Recitals 141–147| CCPA — Section 1798.150

An individual with a cause can seek damages for violation of privacy laws with regard to security measure violations and data

breaches. There is, however, a departure on the judicial remedies available under the legislations. An individual can claim material and nonmaterial damages on any violation of the GDPR,[19] whereas under the CCPA, only on a non-encrypted or non-redacted personal information on being subjected to unauthorised access or exfiltration or theft or disclosure resulting from the business's violation of security obligations is actionable for civil remedies. In such a factual matrix, it is also important for a consumer that prior to initiating any action against a business for statutory damages,[20] a cure period of 30 days be provided to the businesses.[21]

Fines and Penalties

GDPR — Article 83–84 Recitals 148–152| CCPA — Section 1798.155

Both the legislations provide for penalties in cases of noncompliance. While the GDPR provides a list of factors that may aggravate or mitigate the quantum of damages, CCPA does not specifically provide for any such factors. The CCPA has vested the AG with the power of assessing any violation so that a civil action can be brought for the necessary recovery. The amounts set under the legislations are reproduced below:

It is notable that there will be a spate of class actions under CCPA and the penalties for businesses will tantamount to huge amounts as the prescribed penalty is a sizeable amount of upto US$2,500/ US$7,500 for a single count violation.

CCPA: RECENT UPDATES

A. On 11th October, 2019, the California Governor (the Governor), Gavin Newsom, signed into law certain Assembly Bills (AB), which would exempt until 1st January, 2021, from the application of the CCPA. These bills are as follows:
   - AB 25 — such information as is collected by businesses from their employees or contractors,
   - AB 874 — publicly available information and deidentified or aggregate consumer information from the CCPA's application,
   - AB 1202 — which would require data brokers to register with the California AG.

B. Most recently, the US Senate Committee on Commerce, Science and Transportation (the Committee) issued on 3rd December, 2019 a factsheet on a discussion draft of a bill for the United States Consumer Data Privacy Act (USCDPA), laying out the USCDPA's main provisions.[22] The Committee's Chairman, US Senator Roger Wicker, who introduced the draft said that it seeks to provide a Federal Act to establish a national standard for the protection of consumer privacy, combat negative uses of data, require parents' or guardians' opt-in consent for individuals under the age of 16 years before their data can be transferred to a third party, provide the Federal Trade Commission (FTC) with targeted rule-making authority and expand the FTC's authority to cover non-profit organisations and common carriers, as well as grant state AG the authority to enforce its provisions.

It is evident that in the light of the ongoing proposals to revise the CCPA, we

S.No.	GDPR	CCPA
1.	Based on the kind of violations, the penalty may be upto: • 2% of the global annual turnover or €10m, whichever is higher; or • 4% of the global annual turnover or €20m, whichever is higher	Based on the violations, the penalty incurred may be upto: • US$2,500 for each violation • US$7,500 for each intentional violation

may see an 'improved' version of the CCPA and even a Federal Act very soon. Till the time such legislations see the light of the day, however, it is advisable for the businesses within the scope to align their systems and processes with the CCPA. Accordingly, while the Proposed Regulations are in the draft form and open for public consultation, it is advised that businesses commence their compliances in line with these Proposed Regulations simply because they are supplemental in nature to the CCPA and are clarificatory, and the likelihood for them to remain unaltered is very high.

As of today, businesses are faced with a peculiar circumstance. They have aligned their businesses in line with the GDPR and are now also required to align with the obligations under CCPA. While it has been an endeavour to demonstrate that both the legislations do not differ with each other on the core principles of data protection, it is the procedural aspect that has the business taken by storm. While the CCPA comes into effect on 1st January, 2020,[23] the enforcement is to be from 1st July, 2020 onwards. What is crucial to note here is that the CCPA mandates a 'look back' requirement that will require businesses to demonstrate their compliances under the CCPA from 1st January, 2019, onwards.

This entails maintaining records and inventories of personal data of consumers from 1st January, 2019, onwards. While some may argue that CCPA is not compliance intensive in nature due to absence of requirements like data minimising, compulsory filings, data protection authorities, no directions in case of cross-border transactions, it is safe to say that the demonstration of compliances in the past one year has posed unique challenges to the incumbent businesses. The emphasis, therefore, must be on demonstrating and evidencing that the compliances required by CCPA have been done. The privacy policies and contracts, for instance, must be updated regularly, proper disclosures wherever required must be made and the technical capabilities of systems to implement the statutory requirements must be in place.

We have seen most recently that the Digital Advertising Alliance (DAA) announced the publication of tools for the compliance of the advertising industry with the CCPA[24] and the Interactive Advertising Bureau (IAB) issued its CCPA compliance framework and the limited service provider agreement.[25] Industry bodies should lead the path and have in place standardised norms to be followed by their members so as to enable businesses streamline their compliance with the GDPR, the CCPA and other applicable data protection legislations.

It is recommended that compliance of data protection legislations be made a boardroom topic, and the culture of privacy flows from the top to bottom. It is viewed that oftentimes businesses pose financial constraints as an argument of not complying with the data protection legislations. It is urged that the board must understand the criticality of inculcating a culture of data protection and privacy and step in to make appropriate budgetary allocations. Further, thorough and periodical training of stakeholders across business verticals is encouraged and the senior management of the businesses, the marketeers, the sales teams, the finance teams, etc. must attend these trainings to emphasise on the importance of imbibing the culture of privacy as a way of doing businesses. Leadership needs to take cognizance of the fact that the decision of whether to sell personal information is the first step towards achieving compliance with CCPA.

CALIFORNIA PRIVACY RIGHTS ACT (CPRA) — CCPA 2.0?

California voters and legislators have been striving hard to establish a stable and secure data privacy regime for the golden state. In process, CCPA was passed on 28th June, 2018, and became effective from 1st January,

2020. A new ballot measure, Proposition 24, was approved by California voters on 3rd November, 2020, pursuant to which California Privacy Rights Act (CPRA), was passed, effective from 16th December, 2020, and operative from 1st January, 2023.

CPRA is aimed at substantially modifying the current CCPA in order to strengthen its aim and scope, akin to the EU's General Data Protection Act (GDPR). It introduces amendments and adds new provisions to the current CCPA, in relation to protecting California consumer's data privacy, introducing modified obligations on businesses and establishing a new framework for its enforcement via the data protection authority. Although similar to the CCPA, a look back period entails in the CPRA. With 1st January, 2023, as the date of enforcement, it has a look back period from 1st January, 2022. This means that businesses will have to demonstrate their compliances from that time.

This paper analyses important provision of the CPRA and the compliances and obligations that arise from it.

While CPRA was introduced with an aim to secure a stringent and comprehensive data protection regime, a shared aim reflected in the CCPA as well, it majorly expands the nature and tone of the CCPA.

Applicability

Business Threshold

The assessment of gross revenue will be based on the preceding calendar year. The limit set for collection of personal data has been increased to 100,000 from an initial 50,000. Also, entities sharing common control and common branding which share consumer personal information will be now considered as the same 'business'. The reference '*receives* for business's commercial purpose' has been removed from Section California Civil Code §1798.140(d) (B), and it is now limited to businesses that buy, sell and share personal information.

Effective date and operation

- CPRA became effective from 16th December, 2020, and will be in operation from 1st January, 2023; also CPRA Section 25 of the amending act nullifies all previous amendments made to the CCPA, due to which the delay in employee privacy and personal information requirements under the CCPA were nullified.
- Now under Section 145(m), these requirements have been postponed into operation till January 2023. There are, however, two exceptions to it. Under Section 145(m)(3), following two provisions could be interpreted to have taken effect immediately on 16th Decemeber, 2020: the amended California Civil Code §1798.100(a) requiring businesses to issue the expanded 'at collection notices' and the amended California Civil Code §1798.150 providing individuals with a private right of action against businesses for specified security breaches.

Definitional ambit

The CPRA introduces some new definitions while modifying others.

New definitions include 'Advertising and marketing', 'Consent', 'Contractor', 'Cross context behavioral advertising', 'Dark Pattern', 'intentionally interacts', 'Non-Personalized Advertising', 'Profiling', 'Sensitive Personal Information', and 'Sharing'.

Data privacy and governance

Obligation of Business

- Compulsory notices at collection: By amending Section California Civil Code §1798.100, CPRA now imposes a mandatory obligation on businesses which 'control the collection' of consumers' personal data to provide notices to consumers at or before such collection. These pre-collection notices must include

information such as the category of personal/sensitive personal information and the purpose for which it is collected.
- New principles of storage limitation and data minimisation: CPRA introduces concepts of storage limitation and data minimisation by restricting businesses to retain consumer personal data for a period that is 'no longer than necessary' and mandating that collection, retain, sharing, etc. of personal data is specific and limited to what is 'reasonably necessary' for fulfilling the designated purpose
- Contractual obligations: Under California Civil Code §1798.100(d) when sharing or selling personal data, businesses are mandated to enter into contracts with service providers, contractors and third parties with whom personal information is shared or sold to ensure that such data processing and sharing fulfils are compliant with CPRA

Data security and integrity

- CPRA advances on the concept of data security and operational security measures, incorporating them into obligations for businesses. Under Section 100, businesses are required to adopt data security measures and practices, appropriate with the nature of personal data, to ensure that it is protected from security threats such as unauthorised access, data breaches, destruction and modification. This new provision seems to draw inspiration from data security requirements under Article 32 of the GDPR.
- It defines security and integrity as the ability of businesses/data systems to detect and resist personal data from security incidents as well as security incidents and illegal actions and to ensure physical safety. CPRA, thus, now explicitly mandates operational, physical and processing of security requirements.
- By incorporating definitions such as dark patterns, cross-context behavioural advertising and non-personalised advertising, CPRA furthers its control over cybersecurity and data integrity.

Consent

- Opt-in consent has been handled differently in the CPRA. Financial incentive programmes require consumers opt-in consent as per section 999.307(b). While it does not require business to obtain opt-in consent for most of its processing activities, consumers can opt out of sale or sharing of personal information to which they have previously consented to. Section 135(b) explains in detail about consent for sale and use of personal data and the right of the consumer to opt out of such consensual processes.
- Consent itself has been explicitly defined to exclude certain broad and general statements; Section 140(h) states '. . . Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.'

Consumer rights

CPRA has introduced two new consumer rights, namely, right to correct personal information and right to limit use and disclosure of sensitive personal data, while amending certain other rights.

- Right to correction of personal data: Consumers have the right to seek correction from business if the personal information they have is incorrect.
- Right to limit use and disclosure of sensitive personal information*:* Requires that businesses not use or disclose a

consumer's sensitive personal information for purposes other than those necessary to provide the goods or services requested by consumers without providing consumers the right to limit the additional uses or disclosures except for certain limited business purposes. Also, it requires businesses to provide a link to consumers (combined with the opt-out link or separately in a clear and conspicuous manner) reading 'Limit the Use of My Sensitive Personal Information' unless the business allows consumers to opt out via an opt-out preference signal sent with the consumer's consent via a mechanism conforming to specifications to be established by implementing regulations.
- Other rights such as right to delete, opt out of sale, access and nondiscrimination are also available, as under CCPA.
- What is new in CPRA is the waterfall design of fulfilling obligations. Obligations flow from top to bottom approach as evident under section California Civil Codes §1798.105 and 121; these clauses create a waterfall approach for deleting personal data and limiting its personal use. Businesses need to tell their service providers, contractors and third parties who in turn need to contact their service providers and contractors. Presumably, this waterfall continues down the data supply stream until no more additional contracted parties remain.

Enforcement

California Privacy Protection Agency

- Establishes the 'California Privacy Protection Agency' to assume responsibilities for promulgating rules and enforcing the CCPA through administrative proceedings.

Rule-making authority

- Empowers the AG (and eventually the California Privacy Protection Agency) to issue regulations on a wide range of topics, including:
  - Identifying certain 'business purposes' for which service providers may use personal information (on their own behalf);
  - Updating the definition of 'sensitive personal information', 'deidentified' and 'unique identifiers';
  - Establishing when service providers and contractors can combine personal information from multiple sources; and
  - Defining 'specific pieces of information' to minimise delivery of information not helpful to consumers (eg log information and technical data).

Cure period

- Eliminates the 30-day cure period following notice of alleged noncompliance.

Penalty for violations involving minors

- Adds a new penalty of US$7,500 for violations involving personal information of consumers whom the business knows to be under 16 years of age.

ROAD AHEAD FOR GLOBAL BUSINESSES

The moot question facing global business currently is that as CPRA is now passed as a law, do businesses need to start following it or continue to follow the CCPA until 2022?

Effective date and operative date[26]
- Effective date = date on which statue/bill was passed into law
- Operative date = date on which enforcement begins (compliance date)

CCPA timeline
- The state of California vide state bill AB 375 passed 'California Consumer Privacy Rights Act, 2018'.
- The Operative Date for CCPA under AB 375 for CCPA was 1st January, 2020 [Section 1798.198(a)].[27]

- New bill to amend CCPA was passed on vide SB 1121, it delayed the operative date to 1st July, 2020.[28]

CPRA timeline

- Effective date of CPRA was 16th November, 2020.
- Operative date of CPRA is 1st January, 2023.
- Then also, enforcement by newly formed CCP agency will begin from 1st July, 2021, after it assumes charge from California AG.[29]
- Exemption provision pursuant to Sections 1798.145(m) and (n), respectively, are operative immediately (ie from effective date and will become inoperative from 1st January, 2023).[30] Thus, businesses are exempted from application of CPRA and CCPA till 1st January, 2023, with reference to processing and handling employee data and B2B data.
    - The employee information exemption pursuant to 1798.145(m) provides that the CCPA generally does not apply to personal information collected by a business about consumers that are employees, job applicants or owners when that 'information is collected and used by the business solely within the context of' (1) the individual's role as an employee, job applicant, owner, etc., (2) maintaining emergency contact information and (3) the administration of benefits.
    - The B2B exemption provides that the CCPA generally does not apply to personal information collected by a business about an individual consumer when the consumer is acting as an employee on behalf of their employer in the context of 'providing or receiving a product or service to or from' the business.
    - The CPRA extends these CCPA exemptions until 1st January, 2023, effective immediately.

CONCLUSION

From 1st July, 2020, CCPA will be operative and enforceable. Business, however, needs to demonstrate compliance consumer rights under CPRA from 1st January, 2022 (considering the look back period of 12 months from 1st January, 2023), as a consumer's right of access to their data applies to personal information collected by a business on or after 1st January, 2022.

ACKNOWLEDGMENT

My sincere gratitude to Late Mr Kanaya Lal Bazaz, Retired District and Sessions Judge, Jammu & Kashmir, India, for his constant guidance and mentoring.

References and Notes

1. State of California, Department of Finance, The value of goods and services produced in California: Comparison to other major countries', available at: http://www.dof.ca.gov/Forecasting/Economics/Indicators/Gross_State_Product/ (accessed December 2019).
2. The section on 'Right not to be subject to discrimination by virtue of exercise of rights' discusses this right in greater details.
3. The text of the Proposed Regulations, available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf (accessed December 2019).
4. Article 2. Notice to Customers.
5. The Proposed Regulations mandate that at the time of collection of the personal information, the following information must be must be provided to the consumers: (a) a list of the personal information to be collected; (b) the purposes for which each category of personal information will be used; (c) 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 (d) a link to the business's privacy policy or the web address of the business's privacy policy in the case of offline notices.
6. 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.

7. 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.
8. 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.
9. Sec. 999.306(d) of the Proposed Regulations.
10. Article 3 of the Proposed regulations.
11. Article 4.
12. Article 5.
13. Article 6.
14. Sec 999.301(e) of the Proposed Regulations.
15. Sec 999.315 of the Proposed Regulations.
16. There appears to be a discrepancy between Sec 1798.130 and 1798.145 wherein Sec 1798.130(a)(2) of the CCPA allows for an extension of the initial 45-day response period by an additional 45 days, while section 1798.145(g) allows for an extension of the initial 45-day response period by an additional 90 days. The Initial Statement Of Reason (ISOR), Proposed Adoption Of California Consumer Privacy Act Regulations 4 (2019) issued by the Office of the Attorney General states that by adopting the 45-day standard from section 1798.130(a)(2) of the CCPA exclusively, the Regulations have clarified the application of conflicting requirements in the statute.
17. Discussed previously in the section titled 'CCPA: Core Elements'.
18. For instance, as mentioned in Recital 71 to the GDPR: automatic refusal of an online credit application or e-recruiting practices without any human intervention.
19. The GDPR does not guide on any figure for the damages.
20. Damages mandated under the statute require to be an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.
21. Cure period not to operate where the consumer has initiated an action solely for actual pecuniary damages suffered as a result of the alleged violations.
22. The Factsheet- Chairman Wicker's Discussion Draft The United States Consumer Data Privacy Act, available at: https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act (accessed December 2019).
23. As a reprieve to some, a one-year delay in application (01 January 2021) for most of the CCPA requirements has been provided to the following sources of personal information: (1) Personal information collected for purposes of an employment or similar relationship; and (2) Personal information collected and used in business-to-business communications and transactions.
24. Digital Advertising Alliance Announces CCPA Tools for Ad Industry, available at: https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-ccpa-tools-ad-industry (accessed December 2019).
25. IAB Releases the IAB CCPA Compliance Framework for Publishers & Technology Companies and the Limited Service Provider Agreement available at: https://www.iab.com/blog/ccpa-compliance-framework/ (accessed December 2019).
26. '[T]he operative date is the date upon which the directives of the statute may be actually Implemented', in contrast with the effective date which is the 'date upon which the statute came into being as an existing law'. (People v. McCaskey (1985) 170 Cal.App.3d 411, 416; accord, People v. Jenkins (1995) 35 Cal.App.4th 669, 673–674.). Refer: California AG opinion dated 27th January 2020 accessed at: https://oag.ca.gov/system/files/opinions/pdfs/99-1219.pdf (accessed 10th March, 2021)
27. Refer California Assembly Bill No. 375 (CCPA) Section 1798.198 (a) accessed at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375#:~:text=AB%20375%2C%20Chau.,grants%20a%20right%20of%20privacy.&text=The%20bill%20would%20grant%20a%20consumer%20the%20right%20to%20request,a%20verified%20request%2C%20as%20specified (accessed 10th March, 2021)
28. Section 13 of Senate Bill No. 1121 accessed at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (accessed 10th March, 2021)
29. What Comes Next After 'Yes' on 24? From the CCPA to the CPRA and Beyond; Mayer

Brown Legal Update; available at: https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2020/11/cpra-enactment.pdf; also see: What Marketers Need to Know About the California Privacy Rights Act available at: https://www.cmswire.com/digital-marketing/what-marketers-need-to-know-about-the-california-privacy-rights-act/ (accessed 10th March, 2021)

30. See section 1798.145 (m) and (n) of California Civil Code available at: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (accessed 10th March, 2021)