2B Advice®
The Privacy Benchmark

GDPR vs. CCPA

KEY DIFFERENTIATORS YOUR DATA PRIVACY TEAM NEEDS TO KNOW ABOUT CCPA

At a Glance: Understanding How CCPA Compares and Contrasts to the European Union's GDPR.

Privacy regulation is no longer a European Union-only initiative with more and more countries and individual states enacting their own legal framework for the collection and processing of personally identifiable information (PII). One of the more comprehensive data privacy laws to come out of the United States is the **California Consumer Privacy Act (CCPA)** which was passed on June 28, 2018, and is scheduled to go into effect on January 1, 2020. This comprehensive law creates a number of new rights for consumers and considerable compliance concerns for businesses with connections to California and its residents. While some of those new rights and compliance requirements may still be modified in the coming weeks by the California Legislature, there is no doubt that those requirements will be the most comprehensive of their kind outside of the financial and healthcare industries in the United States.

Many of the provisions of the CCPA have been modeled after or been influenced by the **European Union's General Data Protection Regulation (GDPR)**, which is widely considered the gold standard for protecting individual privacy. However, nobody should mistake the CCPA for a "GDPR Light". The CCPA has a distinctly California – style flavor, and many of its requirements have no matching companion provisions in the GDPR. Thus, even for GDPR compliant companies, it is imperative to understand those differences and the requirements of the CCPA in their totality. The time for starting to invest into CCPA compliance is now. As the CCPA requires businesses to account for the PII collected in the 12 months prior to a consumer request, California businesses will have to account already on January 1, 2020 for their use of PII during the year 2019 and not only those data processed after the law's effective date.

This overview is just that, an overview. This is not a comprehensive legal brief on all of the provisions of either CCPA or GDPR and is not meant to be taken as legal advice. Individuals and organizations seeking full compliance with either CCPA or GDPR should consult with qualified advisors. 2B Advice offering its feature-rich privacy management tool 2B Advice PrIME is ready to offer further assistance.

Protected Parties

GDPR

The GDPR protects "data subjects" whose personal data are processed by a data controller established in an EU Member State at the time of data processing or whose data are processed by an off-shore controller offering goods and services or tracking their on-line behavior, provided that such data subjects are physically present in the EU at the time of that processing activity.

CCPA

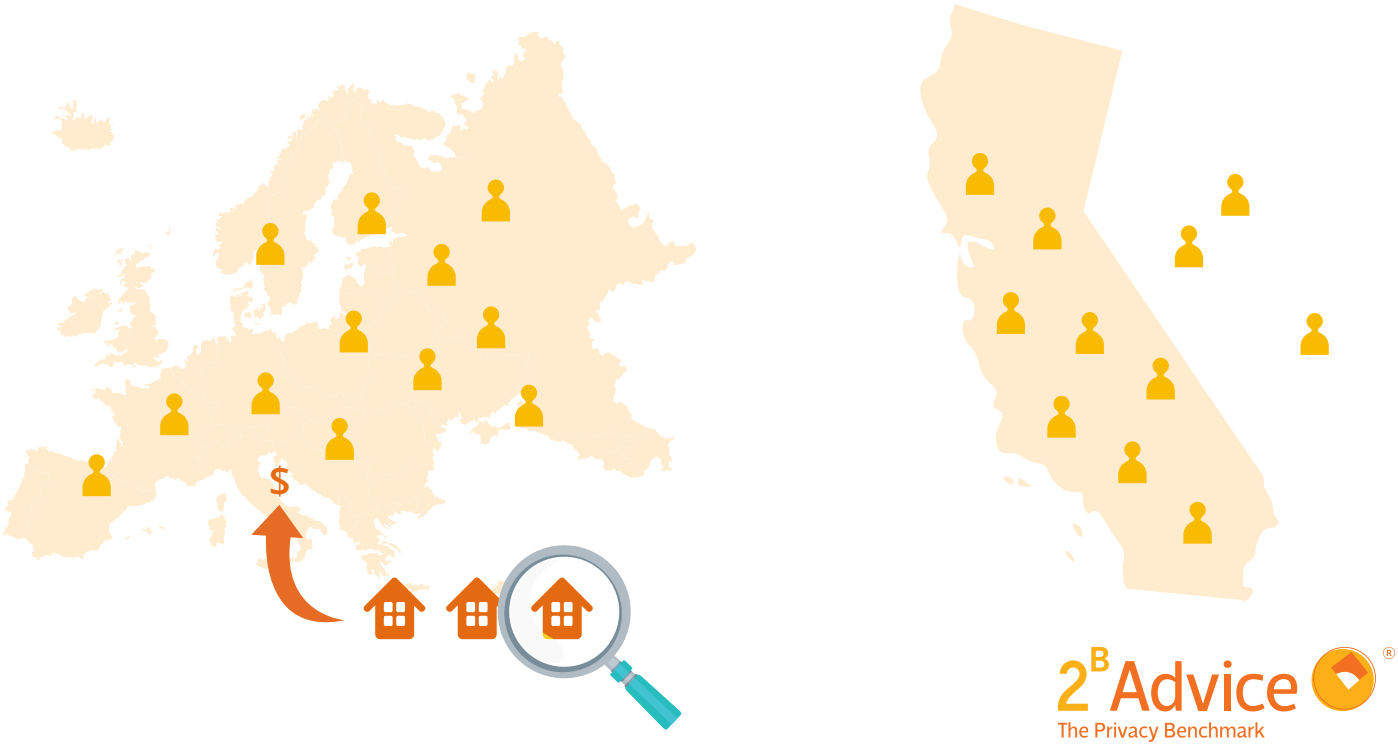
The CCPA protects "consumers" defined as individuals residing in California for purposes other than a temporary or transitory stay whose PII is collected or processed by a business subject to CCPA. As long as individuals remain domiciled in California for tax purposes, they continue to be protected by the CCPA even though they may temporarily use an out-of-state address.

COMPARE AND CONTRAST

Both frameworks consider the location of the covered individuals and the connection of the entities involved in the data processing to the region in which the covered individuals reside.

The GDPR uses a mixed test. Its first prong is asking whether the data controller is established in an EU Member State. Only if that is not the case, the second prong of the test is used to examine whether the data processing activity of an off-shore data controller materially impacts EU residents. Only in that set of circumstances the presence of a data subject in an EU Member State is relevant.

The CCPA focuses on the residency of the consumer while the domicile of the business processing the PII is secondary.



Regulated Entities

GDPR

The term "data controllers" is used in the GDPR to describe private and public bodies that process a data subject's personal data and determine the purpose and means of such processing. Even if data controllers are not established in the EU but in a third country such as the U.S., the GDPR applies if their data processing is associated with offering goods or services to EU residents or monitoring their online behavior while they are physically present in the EU.

CCPA

The CCPA uses the term "businesses", which is defined as all for-profit entities doing business in California that collect and process consumers' personal information and determine the purposes and means of such the collecting and processing. Entities doing business in California will be obligated to comply with the CCPA, if they meet, any one of the three following criteria:

- Sales of consumer's personal information account for at least 50% total annual revenue, or,
- Gross revenues exceed $25 million, or,
- Procurement, sales, or sharing of personal information exceeds 50,000 consumers, households, or devices within one year for commercial use.

The law applies to entities that control or are controlled by a business meeting the above requirements as well as any business sharing common branding with a covered entity.

COMPARE AND CONTRAST

The GDPR is applicable to all public and private sector individuals/entities that process personal data for more than household purposes.

The CCPA is limited in scope to entities that are for profit, meet the specific criteria above, and do business in California.

2B Advice®
The Privacy Benchmark

Additional Regulated Entities

GDPR

In addition to the data controller, the GDPR recognizes the role of the "data processor" as a party that processes personal data on behalf and at the direction of a controller. In their processing activities, data processors must strictly abide by the instructions of the data controller. The GDPR establishes minimum requirements for the contract that a data controller must enter into with a data processor.

Co-controllers and "third parties" are parties other than the original data controller or its processors who may lawfully become engaged in the processing or personal data. In addition, co-controllers who jointly define the means and purposes of a processing activity must allocate their responsibilities in a written agreement.

CCPA

The CCPA distinguishes between "Service Providers" and "Third Parties" as additional parties that may become involved in the processing of consumers' data. Service Providers are for-profit legal entities that process personal information on behalf of a business under a written contract for a predetermined purpose. The written contract that the business and the service provider agree to must forbid the service provider to retain, use, or disclose personal information provided by the business for any purpose other than the business purpose designated in the contract.

Third Parties are defined as entities that receive consumer personal information from the business originally collecting such data but do not meet the description of a service provider. As worded at the time of publication, the CCPA determines that transfers that meet the following criteria are considered exempt:

- Data authorized or requested by the consumer
- Data used to alert a third party of opt-outs
- Data used to notify a defined "Service Provider
- Data in transactions where the receiver of data assumes control of the business/transaction.

Third Parties who do not meet this criteria have independent obligations in regards to consumers such as providing consumers with an explicit notice and an opportunity to opt-out before their personal information is re-sold to another business.

COMPARE AND CONTRAST

There are significant differences in the definition of data processors and service providers and what conditions must be met under each framework before data can entrusted for processing to such entities.

The GDPR has specific and more detailed mandates than the CCPA as to what terms need to be included in the written agreement a third party must sign to qualify as a data processor. In addition, also parties jointly controlling a processing activities must sign an agreement as co-processors to ensure that the rights of the data subjects are fully protected.

The CCPA focuses on the concept of "sale of PII" and "disclosure for business purposes" and privileges certain third party recipients of PII that enter into a service provider agreement.

2B Advice®
The Privacy Benchmark

Protected Data

GDPR

The GDPR defines information that is protected as "personal data", which is any information relating to an identified or identifiable natural person, including:

- Names
- Identification numbers
- Location data
- Online identifiers
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

CCPA

The CCPA defines information that is protected as "personal information", which identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household. Some of the categories of personal data include (but are not limited to):

- Legal Name
- AKAs (aliases)
- Mailing Address
- Email Address
- Unique online persona
- IP Address
- Name on accounts
- Government ID Information including Driver's Licenses and Passports
- Physically identifiable traits
- Education (when included with other PII)
- Medical Information not excluded by HIPAA already
- Financial information not excluded by financial regulations already
- Protected classes (when included with other PII)
- Biometric data (when included with other PII)
- Online activity (when included with other PII)
- Geolocation (when included with other PII)
- Employment information (when included with other PII)
- Other inferences drawn from preferences, predispositions, behaviors, etc. (when included with other PII)
- Household data

Excluded from this definition:

- Deidentified data
- Aggregate data
- Federal records
- State records
- Local Government records
- Medical information already regulated by State and Federal law
- Clinical trial information already subject to Federal Policy on Human Subjects
- PII regulated by Fair Credit Reporting Act (FCRA)

COMPARE AND CONTRAST

The GDPR takes a more conceptual approach to PII whereas the CCPA has very specific definitions in place for what is and isn't covered. Both regulations mention anonymous data and do not consider it PII, however, the requirements of each regulation are considerable.

The GDPR is an universal privacy regulation without any sectoral carve-outs by its terms equally enforceable in every EU Member State.

The CCPA is only one of the U.S. frameworks to afford consumers some protection of their privacy. Consumers must also be aware of their rights under a multitude of other laws, e.g. HIPAA or GLBA to fully protect their privacy interests.

2B Advice®
The Privacy Benchmark

Right to Notification

GDPR

The GDPR mandates that the data controller communicates detailed information about its data collection and processing practices. To paraphrase, certain key requirements, a data controller must inform the data subject of the following:

- The purpose for processing personal data.
- The legal basis for processing personal data
- The categories of personal data that will be collected and processed.
- Who the recipients of their personal data are.
- The contact details of those processing their data.
- If the personal data will be transferred to a third country.
- The period that the personal data will be stored.
- The existence of automated decision-making.
- All of the data subject's rights defined by the GDPR.

CCPA

Businesses are obligated to inform consumers at or before the point of collection of personal information what categories and purpose of the personal information will be collected. Businesses must provide additional notice before collecting additional categories or using the personal information for a different purpose. Specific disclosures must be included in businesses' privacy policies.

COMPARE AND CONTRAST

GDPR and CCPA differ significantly in their approach to data collection disclosure.

The GDPR utilizes the concept of legal basis as well as notification and disclosure of recipients. Additionally, the GDPR requires a disclosure of any cross border transfer of data as well as contact details of data processors.

The CCPA mandates consumer disclosure at or before collection of personal information and requires businesses to disclose additional data collection at future dates, it does not require a "legal basis" for the collection of data. As such, the agreement is between the consumer and the company and is governed by the business' privacy policies.

2B Advice®
The Privacy Benchmark

Security Requirements

GDPR

The GDPR requires data controllers and processors to implement technical and organizational measures (TOMs) to ensure the reasonable safety of their data processing operations. The GDPR adopts a risk-based approach to determine what level of technical and organizational measures are required in each case. Relevant factors include the nature and volume of the data processing activities, criticality of the data processed and the risks associated with the specific processing operations.

CCPA

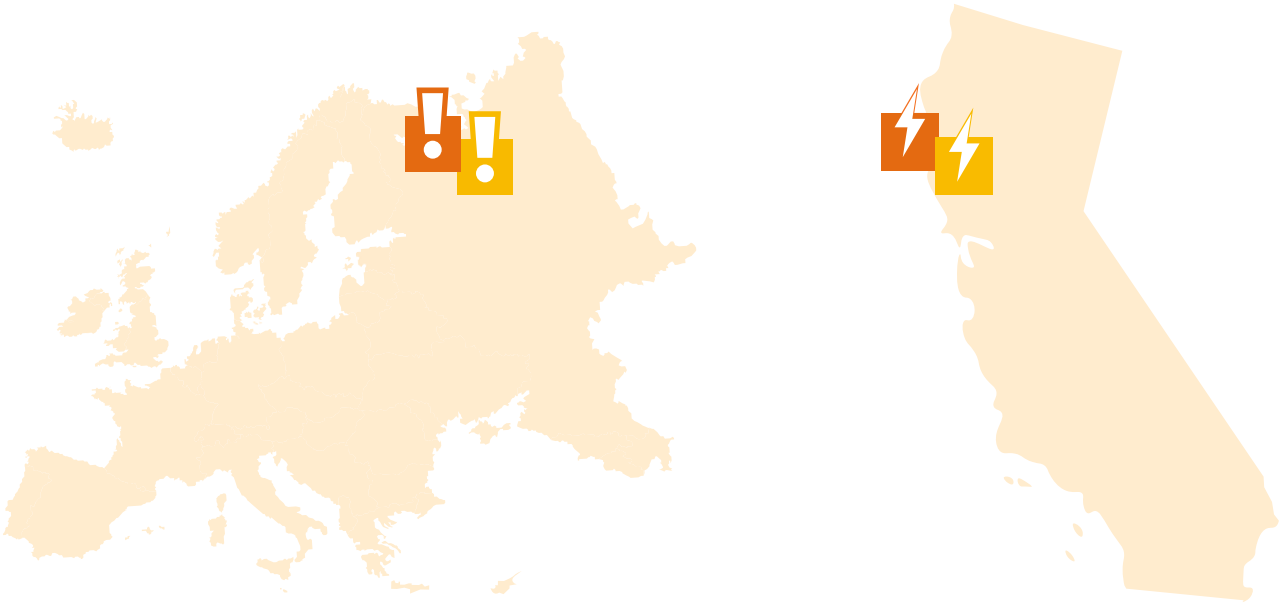
The CCPA does not contain any explicit provisions requiring businesses to implement a certain level of security measures. However, the CCPA provides for a limited private right of action in case of data breaches involving unencrypted or non-redacted personal information, caused by the failure to uphold reasonable security measures to manage risk at an appropriate level.

COMPARE AND CONTRAST

The GDPR, however, requires data controllers and data processors to have defined Technical and Organizational Measures (TOMs) in place to ensure the reasonable safety of their data processing activities. Rather than being reactive, GDPR attempts to take a proactive approach to data security.

The CCPA and the GDPR take vastly different approaches to ensuring data security.

The CCPA neither defines nor regulates data security. Rather, it provides that, in case of a data breach, businesses that lack "reasonable security measures" are subject to a private right of action.



2B Advice®
The Privacy Benchmark

Right to Opt-out

GDPR

The GDPR grants the right to withdraw consent from processing activities as well as to object to processing for marketing purposes also in cases where the data controller does not rely on consent.

CCPA

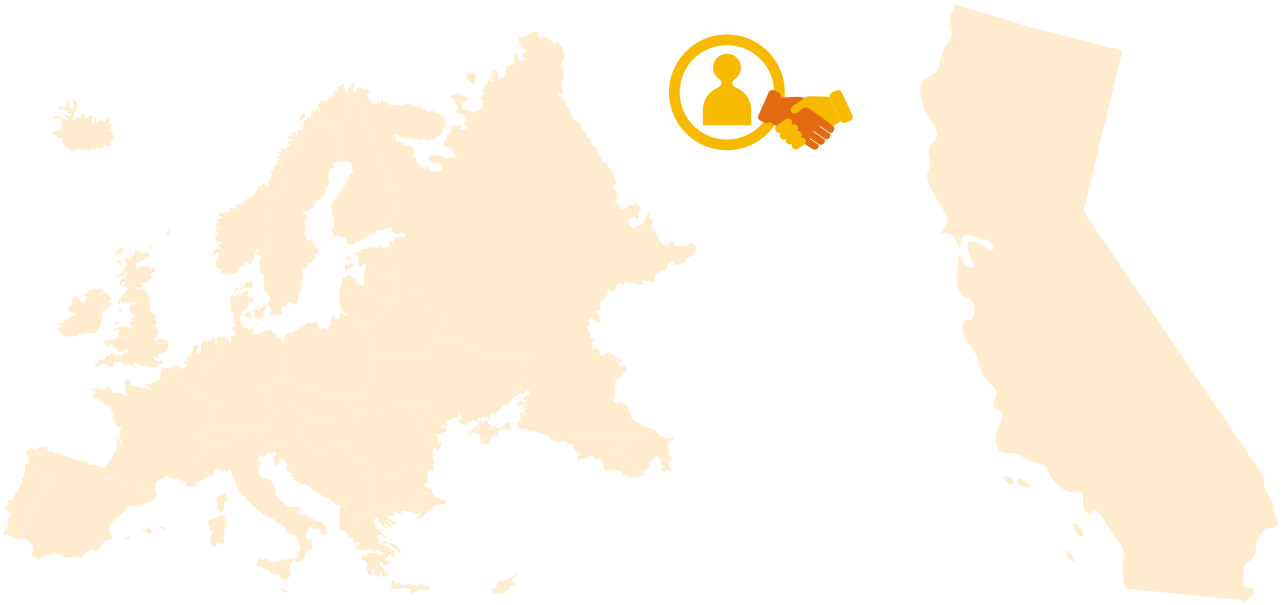
Businesses must comply with consumers' requests to cease from selling (as defined under CCPA as a "sale") their personal information to third parties. To facilitate the exercise of those consumer rights, businesses must, among other things:

- Implement the organizational and technical requirements to be able to comply with such consumer requests
- Include on their website a clear and conspicuous "Do Not Sell My Personal Information" link for consumers to exercise their rights.

COMPARE AND CONTRAST

The GDPR does not provide for a separate right to exclude businesses from selling personal data. However, withdrawing consent for processing activities or objecting to processing for marketing purposes offers a comparable level of protection for data subjects.

The CCPA attempts to outline the use of data outside of the organization collecting that data and give the consumer rights to refuse the monetization of their data even when no actual money is exchanged.



2B Advice®
The Privacy Benchmark

Protection for Minors

GDPR

The GDPR designates rules for minors in regards to offers of information society services to children. The GDPR allows Member States to designate a minimum age for consent as long as the age is no lower than 13 years of age. However, by default the age of consent is 16 years of age. If the data subject is below the age of consent in the particular Member State then their legal guardians must grant consent.

CCPA

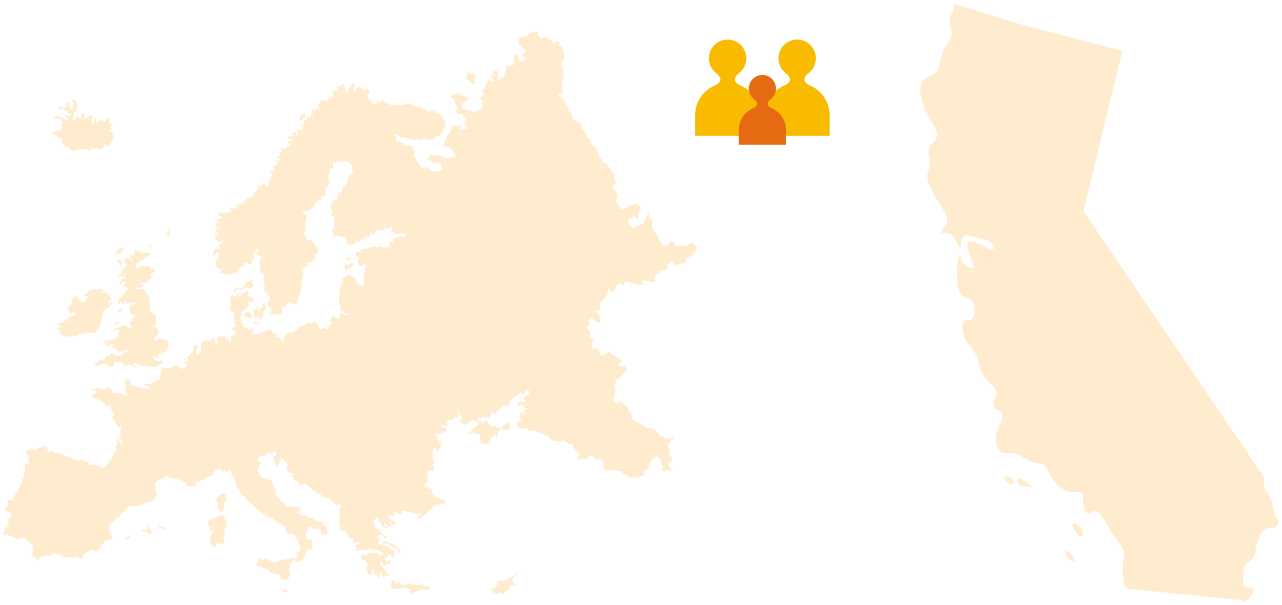
The CCPA forbids any sales of personal information pertaining to consumers under 16 years of age without consent. Between the ages of 13 and 16 children can consent by opting-in to be able to consent. Below age 13, businesses wishing to process personal information of children are required to obtain parental consent.

COMPARE AND CONTRAST

Both regulations do not allow for the collection of data of any kind for minors under the age of 13 without legal guardian consent.

The GDPR considers the age of consent to be 16 unless otherwise determined in a given member state, with the minimum age of consent being 13.

In the case of CCPA, however, minors between the ages of 13 and 16 can consent to the disclosure of their PI to third parties ("opt-in").



2B Advice®
The Privacy Benchmark

Disclosure/Portability

GDPR

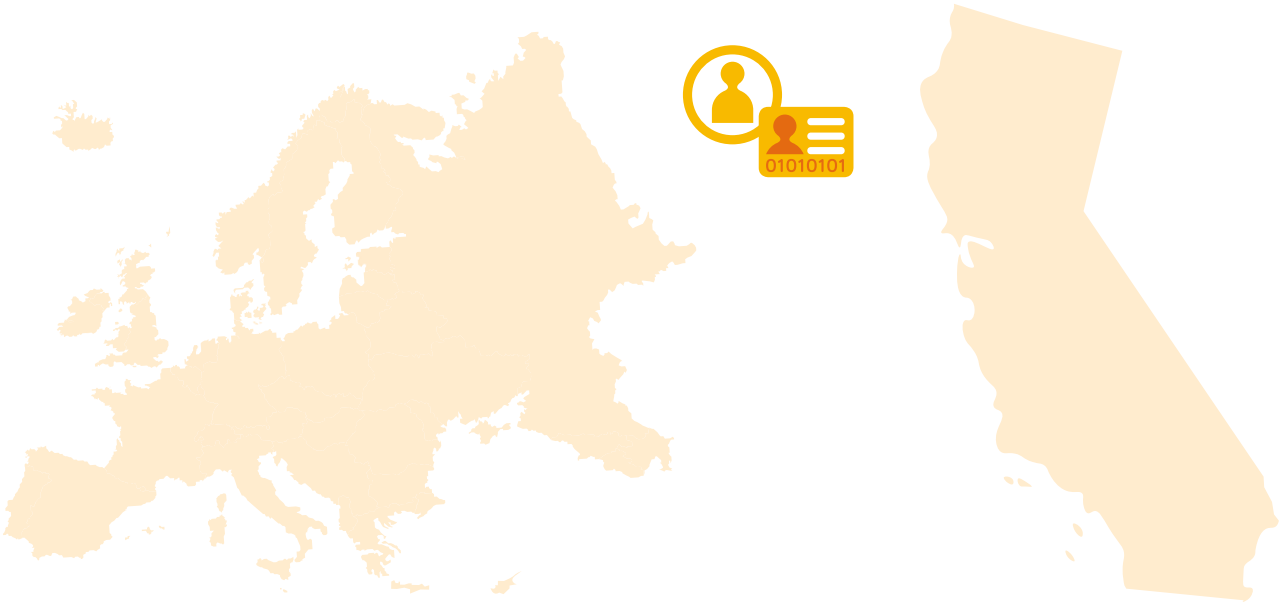
The GDPR grants data subjects the right to have access to their personal data, including additional information on the data controller's processing activities. Data subjects have the right to receive this information in a structured, machine-readable format to facilitate the transfer of information to other entities the consumer wishes to send it to without barriers.

CCPA

Consumers have the right to have their personal information disclosed to them, both in terms of the categories of information collected with respect to them but also with respect to the specific pieces of information held by the business with respect to them. The relevant information must be disclosed in a readily usable format to facilitate, without barriers, the transfer of information to wherever the consumer wishes to send it to. Consumers must also be notified about the business's purpose for using their personal information as well as which third parties the information will be shared with.

COMPARE AND CONTRAST

The GDPR and CCPA both provide for PII that is collected being disclosed to the consumer in a readily usable format (structured, machine-readable format) that allows the individual to transfer it to another party (CCPA) respectively require the data controller to transmit the personal data directly to a new controller if technically feasible (GDPR).



2B Advice®
The Privacy Benchmark

Erasure

GDPR

Data controllers must comply with data subject's requests of erasure of their personal data only in certain scenarios (see below).

- The personal data is no longer necessary to fulfill the purpose on why it was collected.
- The data subject withdraws consent and their personal data is within a special category of data, while there is no other legal ground for processing.
- The data subject objects to the processing pursuant to direct marketing purposes.
- The personal data was processed unlawfully.
- The personal data is required to be erased to comply with legal obligations to other EU or Member State law.
- The collection of the personal data relates to the offer of information society services.
- A part of complying with the data subject's request is that the data controller must direct any relevant data processors to delete the subject's personal data as well.

CCPA

Businesses must comply with consumer's requests for deletion of their personal information, with certain exceptions. A consumer's deletion request does not only affect the personal information held by the respective business directly but also requires the respondent business to reach out to its service providers and require the same to delete any relevant data covered by the consumers' request.

COMPARE AND CONTRAST

The GDPR has very specific criteria in which a data subject must make a request for the deletion of data and the ability to refuse is much more narrowly defined within the GDPR.

The CCPA has broad rights for consumers seeking to delete their data, however, the CCPA also allows for much broader reasoning for refusing such requests.

2B Advice®
The Privacy Benchmark

Rectification

GDPR

Data subjects have the right to request to data controllers to correct inaccurate personal data and complete incomplete personal data.

CCPA

Consumers have no legal recourse for correcting data under CCPA.

COMPARE AND CONTRAST

The GDPR and the CCPA are very different in regards to the right to rectification.

The GDPR, however, has guidelines in place to allow data subjects to correct any erroneous data a data controller may have on file.

With no provision for rectification, the CCPA is lacking in regards to incorrect data a company may have on file. However, there may still be recourse through the request to delete any data related to a consumer.

2B Advice®
The Privacy Benchmark

Restrictions on Processing

GDPR

Data Subjects may request the restriction of their PII by objecting to:

- Direct marketing
- Statistical research
- Scientific research
- Historical research
- Automated decision making such as profiling

CCPA

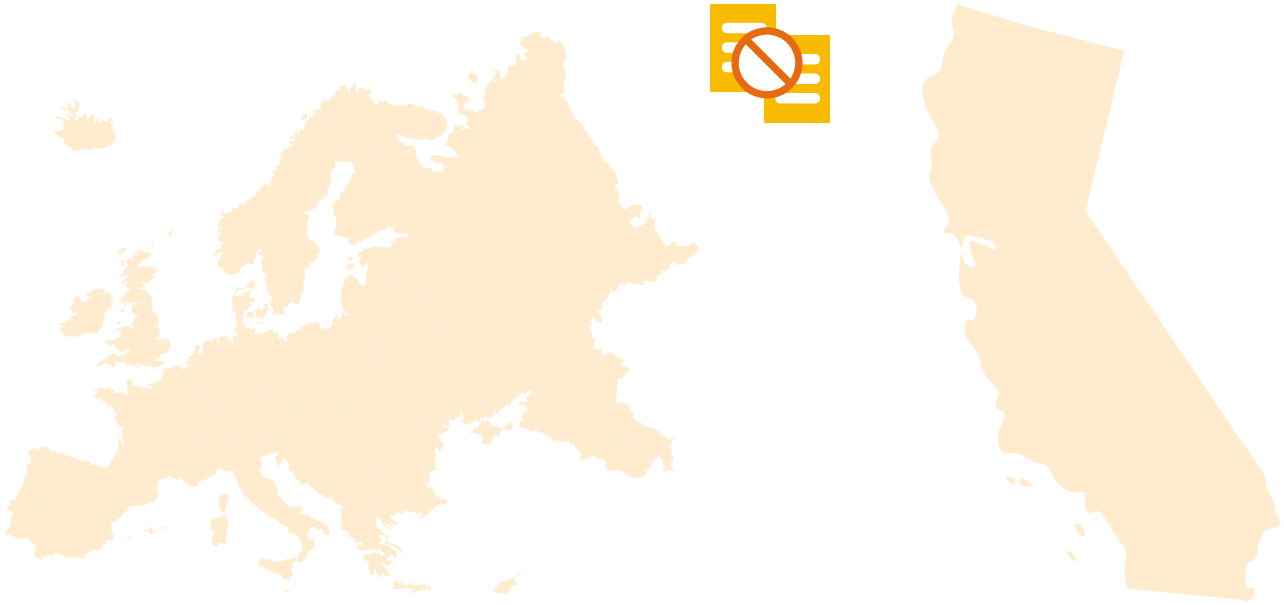
Consumers do not have the ability to restrict processing of their PII. However, they may restrict data being sold to third parties or may request deletion of PII.

COMPARE AND CONTRAST

There are limitations in how PII can be restricted in both the GDPR and the CCPA.

Under the GDPR, a data subject may request restriction based on specific criteria.

In order to restrict processing of data under the CCPA, a consumer must restrict the sale to third parties or request the full deletion of PII



2B Advice®
The Privacy Benchmark

Non-Discrimination

GDPR

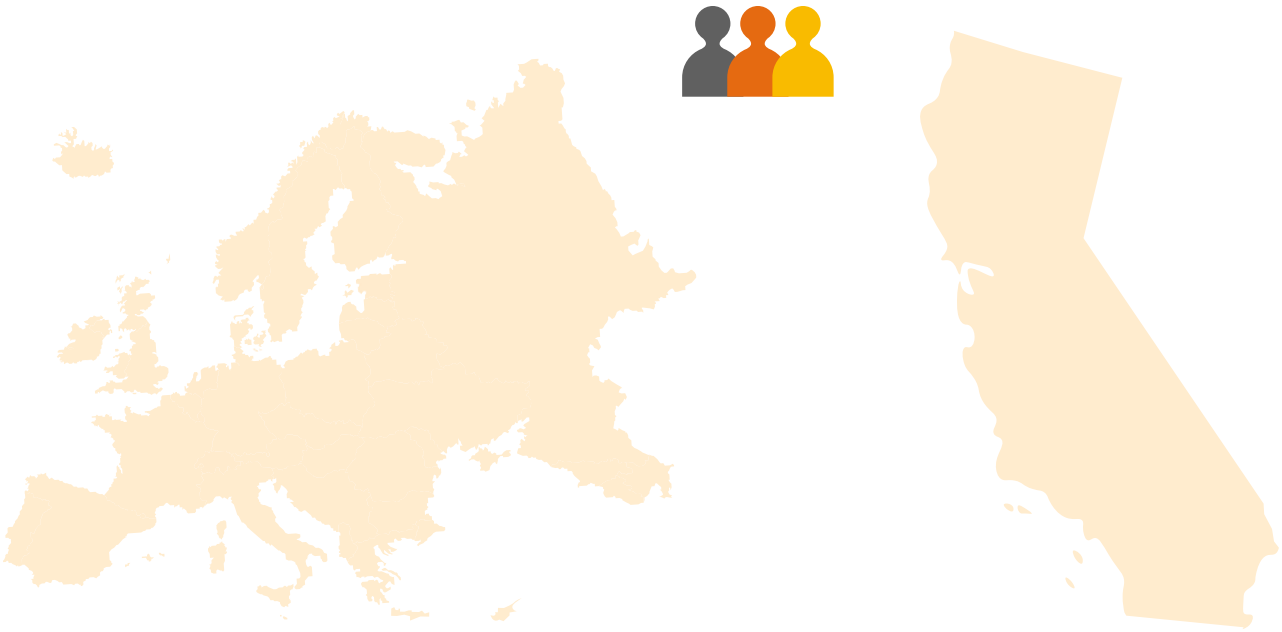
Data controllers are prohibited from discriminating against data subjects based on exercising their rights, e.g., the tying of certain benefits to a data subject consenting to data processing not strictly necessary under the circumstances. In addition, the GDPR's protections against automated individual decision-making including profiling, aims, among other things, at protecting data subjects against discrimination based on their personal characteristics.

CCPA

Businesses are prohibited from discriminating against consumers based on exercising their rights under the CCPA, yet a business may offer different pricing or financial incentives to certain consumers based on the value derived from being allowed to process the personal information of such consumers.

COMPARE AND CONTRAST

The GDPR approaches the problem on the level of processing activities while the CCPA merely attempts to blunt the discriminatory effects of certain business practices. As there are several amendments pending that attempt to clarify or re-shape the scope of the non-discrimination obligations flowing from the CCPA, the jury is still out on how the two frameworks stack up against each other.



2B Advice®
The Privacy Benchmark

Information Requests

GDPR

Data controllers must respond to any requests from data subjects seeking to vindicate their individual rights under the GDPR. Data controllers must comply with a data subject request after identity verification by responding within a month (potentially extendable for two additional months). The data controller may charge a reasonable fee based on administrative costs.

CCPA

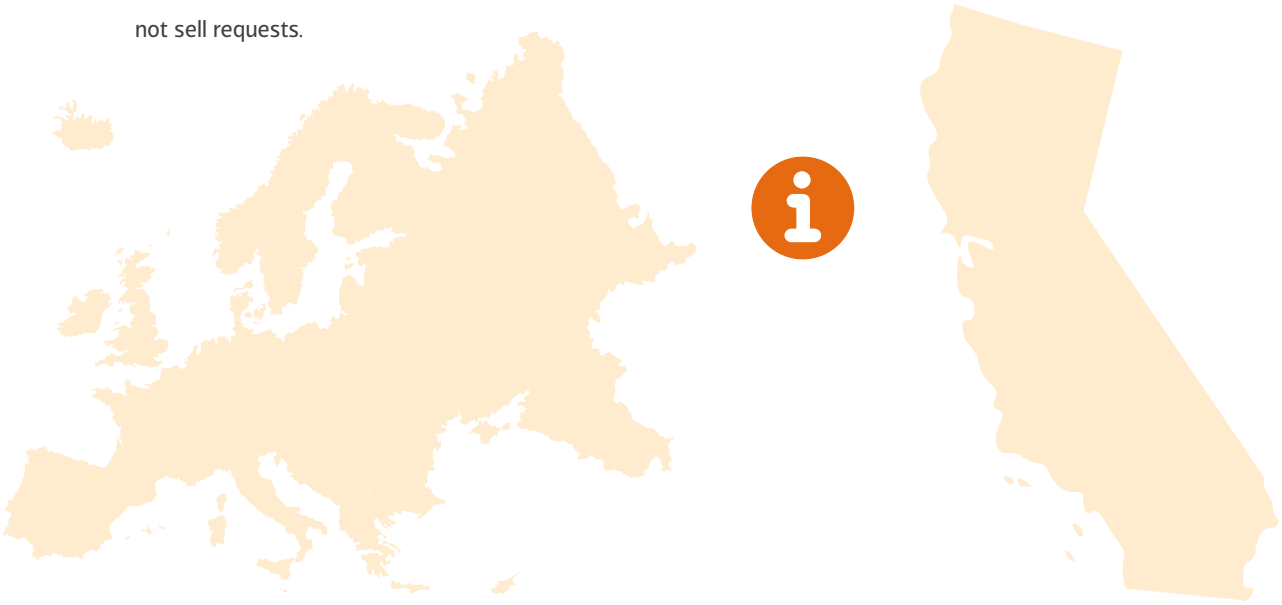
Unless a consumer request is manifestly unfounded, businesses must comply with consumer's request after identity verification by responding within the 45 day time allotment (time allotment is potentially extendable to 90 days). Even if the business chooses not to comply with the consumer's request, they must provide the reasons for not doing so. Consumers are restricted to only two information requests per year, with no limitations on deletion and do-not-sell requests.

COMPARE AND CONTRAST

Both the GDPR and the CCPA allow an individual to make information requests, and they are very similar in overall timelines.

Under the GDPR, the timeline for response is similar to the CCPA (no more than 90 days after request for extension). Also, it is important to note that a data controller may charge a reasonable fee based on administrative costs.

Under the CCPA, a consumer must receive the data no later than 90 days from request if an extension is requested by the business. Additionally, a business may provide reasons for denying a request should they choose to do so. Another consideration is that only two information requests may be made by a single consumer to a given business every 12 months. However, this does not stop the consumer from making any number of deletion and do not sell requests.



2B Advice®
The Privacy Benchmark

Enforcement and Fines

GDPR

Data subjects may choose between lodging complaints with the competent Supervisory Authorities or bring a legal action in a national court to vindicate any violations of their rights under the GDPR. EU Member States can charge civil penalties reaching up to 20 million Euro or 4% annual global revenue, whichever is highest. In addition, EU Member States may also issue administrative fines and take other enforcement steps such as seizure of processing equipment or issue C&D orders.

CCPA

Certain data breaches allow consumers a private right of action to seek actual damages or statutory damages ranging from USD $100 to $750 per incident, in junctive or declaratory relief or any other relief a court deems proper. There is no cure period to allow the business to come into compliance in case of an individual claim for actual damages, however, in case of an intended class action, the offending business is entitled to a 30 day cure period.

The California Attorney General (AG) may fine businesses USD $2,500 to $7,500 per violation, if intentional. However, also in this case, a 30-day cure period is granted. It is important to note that currently the California AG is not mandated to begin enforcement until July of 2020.

COMPARE AND CONTRAST

The penalties for non-compliance for both the GDPR and the CCPA can be considerable when tallied in full.

Under the GDPR, the fines that can be levied by a DPA are limited to the greater of 4% of annual revenue or 20 Million Euros (whichever is larger). For large companies this can mean fines in excess of $100 Million (as evidenced by the ICO fine against British Airways).

The size of penalties under the CCPA is relatively small when considered on an individual infraction level, however, could become considerable in cases where large groups of consumers are affected and multiple infractions are made. As such, the penalties could be considerable and far beyond those of the GDPR though this is unlikely in practice.

2B Advice®
The Privacy Benchmark

Conclusion

Both the GDPR and the CCPA are comprehensive privacy laws that seek to protect the residents of their prospective boundaries. GDPR is more conceptual in nature and applies to more than just for-profit organizations, and as such, has become the gold standard for privacy compliance. While CCPA is not as comprehensive in scope, it does have specific, considerable additional parameters that help to protect its consumers. As such, the fast approaching effective date for CCPA is important to executives and their privacy and security teams are looking for ways to address its additional requirements. CCPA is likely just the beginning for U.S. based companies as other state and federal privacy regulations are passed and begin to take shape. It is the time to set up the additional processes and systems that are inherent best data privacy practices and compliance.

If you are looking for support in people, processes, or technology surrounding privacy compliance, reach out to 2B Advice at (858)366-9753 or email us at sandiego@2b-advice.com. 2B Advice brings over 16 years of people, process, and technology in addressing global privacy compliance requirements. How can we help you?

2B Advice®
The Privacy Benchmark

Glossary of Terms

Another similarity the CCPA has with the GPDR is the extensive use of regulation-specific terminology. The CCPA GDPR comparison has used many of those CCPA terms. Below is a glossary of terms.

Age of Consent: The age at which a consumer is able to freely give a specific, informed, and unambiguous indication of his or her wishes, conveying an agreement to the processing of personal data relating to him or her.

AG: Attorney General. The main legal advisor to a government who often has overview of law enforcement.

Aggregate Consumer Information: Information pertaining to a group or category of consumers that cannot be linked or reasonably linkable to consumers or households by removing individual consumer identities.

CCPA: The California Consumer Protection Act

Controls: The administrative, technical, management, or legal means of managing risk, including policies, procedures, guidelines, practices or organizational structures.

Cure Period: A period of time a business or service provider may use to try to rectify the violations of the CCPA that could result actual or statutory damages or civil penalties.

Data Controller: An entity that determines the purpose and means of processing personal data, alone or jointly.

Data Processor: An entity that processes personal data on behalf of a data controller.

Data Subject: A natural person that can be identified, directly or indirectly, by reference to an identifier.

Deidentified: All identifiers that have been disconnected from the dataset. Although, a separate file may exist showing the connection between the identifiers and the data in question.

GDPR: The General Data Protection Regulation.

Household Data: Data pertaining to a household as a whole, rather than data attributable to individuals of a household.

Information Society Services: eCommerce sites, live or on-demand streaming services, or organizations providing or providing access to communication networks.

Measure: A task or action that are used to mediate data privacy risks.

Personal Information: Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. There are 11 categories of identifiers that the CCPA lists, however, the CCPA does not limit what is considered personal information to what is contained in that list. Any publicly available information is not considered personal information.

Pseudonymization: A method of processing personal data that no longer allows data to be associated with a specific data subject, without having to utilize additional information.

Publicly Available Information: Information lawfully made available by federal, state, and local government records.

Rectification: Correcting inaccurate information.

Reidentification: Reversing the deidentification process by connecting data with the identity of a particular consumer.

Service Provider: A for-profit legal entity that receives personal information from a business and processes information on behalf of a business under written contract that forbids storing, using, or disseminating personal information for purposes outside of what is included in the contract.

Third Party: A party that to which another business discloses personal information for business purposes but does not qualify as a Service Provider. This is somewhat comparable to a data controller receiving data from another data controller in GDPR terms.

TOMs: An acronym for Technical and Operational Measures. The functions, procedures, and measures manufactured to protect personal information that an organization processes.

2B Advice®
The Privacy Benchmark

2B Advice®
The Privacy Benchmark

2B Advice LLC
7220 Avenida Encinas, STE 208
Carlsbad, CA 92011, USA
Phone_ +1 (858) 366-9750
sandiego@2b-advice.com

2B Advice GmbH
Bonn - Berlin - Munich, Germany
Vienna, Austria
Verona, Italy
Paris, France

2B Advice s.r.o.
Brezno, Slovakia

www.2b-advice.com